SnapManager 3.4.2 para Oracle

SnapManager Oracle

NetApp
June 20, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapmanager-oracle/index.html on June 20, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

SnapManager 3.4.2 para Oracle . . . 1
Notas de la versión de SnapManager 3.4.2 para Oracle . . . 2
Guía de instalación y configuración para UNIX® . . . 3
- Información general del producto . . . 3
  - Aspectos destacados de SnapManager . . . 3
  - Arquitectura SnapManager . . . 4
- Flujo de trabajo de implementación . . . 5
- Preparación para la implementación . . . 6
  - Licencias de SnapManager . . . 7
  - Configuraciones admitidas . . . 8
  - Tipos de almacenamiento admitidos . . . 8
  - Requisitos del host UNIX . . . 9
- Configurar bases de datos . . . 9
  - Configurar la base de datos de destino . . . 9
  - Crear un usuario de base de datos de Oracle para la base de datos de destino . . . 9
  - Crear la instancia de la base de datos del repositorio . . . 10
  - Crear un usuario de Oracle para la instancia de la base de datos del repositorio . . . 10
  - Verificación de la configuración del listener de Oracle . . . 11
- Instalando SnapManager . . . 11
- Configurar SnapManager . . . 12
  - Iniciando el servidor SnapManager . . . 12
  - Obtener acceso a la interfaz de usuario de SnapManager . . . 12
  - Configurar el repositorio de SnapManager . . . 13
- Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault . . . 14
  - Comprender las diferencias entre SnapMirror y SnapVault . . . 15
  - Preparar los sistemas de almacenamiento para la replicación de SnapMirror . . . 15
  - Preparar sistemas de almacenamiento para la replicación de SnapVault . . . 17
- Realizar backup y verificación de las bases de datos . . . 19
  - Información general sobre backup de SnapManager . . . 19
  - Definición de una estrategia de backup . . . 20
  - Crear un perfil para la base de datos . . . 22
  - Realizar una copia de seguridad de la base de datos . . . 25
  - Verificación de los backups de las bases de datos . . . 27
  - Programación de copias de seguridad periódicas . . . 27
- A continuación, ¿dónde ir . . . 29

Guía de instalación y configuración para UNIX® . . . 31
- Información general del producto . . . 31
  - Aspectos destacados de SnapManager . . . 31
  - Arquitectura SnapManager . . . 32
- Flujo de trabajo de implementación . . . 34
- Preparación para la implementación . . . 35
  - Licencias de SnapManager . . . 35
  - Configuraciones admitidas . . . 36

Tipos de almacenamiento admitidos . . . 36
Requisitos del host UNIX . . . 37
Configurar bases de datos . . . 37
Configurar la base de datos de destino . . . 37
Crear un usuario de base de datos de Oracle para la base de datos de destino . . . 37
Crear la instancia de la base de datos del repositorio . . . 38
Crear un usuario de Oracle para la instancia de la base de datos del repositorio . . . 38
Verificación de la configuración del listener de Oracle . . . 39
Instalando SnapManager . . . 39
Configurar SnapManager . . . 40
Iniciando el servidor SnapManager . . . 40
Obtener acceso a la interfaz de usuario de SnapManager . . . 40
Configurar el repositorio de SnapManager . . . 41
Realizar backup y verificación de las bases de datos . . . 42
Información general sobre backup de SnapManager . . . 43
Definición de una estrategia de backup . . . 43
Crear un perfil para la base de datos . . . 45
Realizar una copia de seguridad de la base de datos . . . 48
Verificación de los backups de las bases de datos . . . 50
Programación de copias de seguridad periódicas . . . 50
A continuación, ¿dónde ir . . . 52
Guía de administración para UNIX® . . . 54
Información general del producto . . . 54
Aspectos destacados de SnapManager . . . 54
Crear backups usando copias de Snapshot . . . 55
Por qué debe prune los archivos de registro de archivos . . . 55
Consolidación de registros de archivo . . . 56
Restauración total o parcial de bases de datos . . . 56
Comprobar el estado del backup . . . 56
Clones de backups de bases de datos . . . 56
Realizar un seguimiento de los detalles y generar informes . . . 57
Qué repositorios son . . . 57
Qué perfiles son . . . 58
Qué son los estados de operación de SnapManager . . . 60
Cómo mantiene SnapManager la seguridad . . . 61
Acceso e impresión de la Ayuda en línea . . . 62
Diseños generales de bases de datos y configuraciones de almacenamiento recomendados . . . 62
Limitaciones al trabajar con SnapManager . . . 75
Crear backups usando copias de Snapshot . . . 83
Por qué debe prune los archivos de registro de archivos . . . 83
Consolidación de registros de archivo . . . 83
Restauración total o parcial de bases de datos . . . 84
Comprobar el estado del backup . . . 84
Clones de backups de bases de datos . . . 84
Realizar un seguimiento de los detalles y generar informes . . . 85

Qué repositorios son . . . 85
Qué perfiles son . . . 86
Qué son los estados de operación de SnapManager . . . 88
Eventos recuperables e irrecuperables . . . 88
Cómo mantiene SnapManager la seguridad . . . 89
Acceso e impresión de la Ayuda en línea . . . 90
Diseños generales de bases de datos y configuraciones de almacenamiento recomendados . . . 90
Definir el inicio de la base de datos con el archivo oratab . . . 91
Requisitos para usar bases de datos de RAC con SnapManager . . . 92
Requisitos para usar bases de datos de ASM con SnapManager . . . 92
Dispositivos de partición compatibles . . . 93
Compatibilidad con ASMLib . . . 94
Compatibilidad con bases de datos de ASM sin ASMLib . . . 95
Requisitos para usar bases de datos con NFS y SnapManager . . . 100
Ejemplos de distribuciones de volúmenes de base de datos . . . 101
Limitaciones al trabajar con SnapManager . . . 103
Limitaciones de SnapManager para Clustered Data ONTAP . . . 109
Limitaciones relacionadas con Oracle Database . . . 109
Restricciones en la gestión de volúmenes . . . 110
Actualizar SnapManager . . . 111
Preparando la actualización de SnapManager . . . 111
Actualizar los hosts SnapManager . . . 111
Tareas posteriores a la actualización . . . 112
Actualizar hosts de SnapManager mediante actualización gradual . . . 114
Configurando SnapManager . . . 122
Parámetros de configuración de SnapManager . . . 122
Configuración de SnapDrive para UNIX para un entorno activo/activo de Veritas SFRAC . . . 131
Configurar SnapManager para que sea compatible con el entorno de Veritas SFRAC . . . 131
Asegurarse de que ASM detecta discos importados . . . 132
Seguridad y gestión de credenciales . . . 133
Qué es la autenticación de usuario . . . 134
Acerca del control de acceso basado en roles . . . 135
Almacenamiento de contraseñas cifradas para secuencias de comandos personalizadas . . . 140
Autorizando el acceso al repositorio . . . 141
Autorizando el acceso a los perfiles . . . 141
Visualización de las credenciales de usuario . . . 141
Borrar credenciales de usuario para todos los hosts, repositorios y perfiles . . . 142
Eliminación de credenciales para recursos individuales . . . 143
Gestionar perfiles para backups eficientes . . . 144
Tareas relacionadas con perfiles . . . 144
Acerca de los perfiles y la autenticación . . . 144
Creación de perfiles . . . 145
Nomenclatura de copias Snapshot . . . 152
Cambiar el nombre de los perfiles . . . 154
Cambio de contraseñas de perfil . . . 154

Restablecimiento de la contraseña del perfil . . . 155
Autorizando el acceso a los perfiles . . . 155
Verificando perfiles . . . 155
Actualizando perfiles . . . 156
Eliminar perfiles . . . 161
Realizar backups de bases de datos . . . 161
Qué son los backups de la base de datos SnapManager . . . 163
Qué son los backups completos y parciales . . . 163
Acerca del manejo de archivos de registro de archivo y archivos de control . . . 169
Qué es la programación de backups de base de datos . . . 170
Creación de backups de la base de datos . . . 174
Qué es AutoSupport . . . 188
Verificación de los backups de las bases de datos . . . 189
Cambiar la política de retención de backups . . . 190
Ver una lista de backups . . . 192
Ver los detalles de backup . . . 192
Montar backups . . . 193
Desmontaje de backups . . . 194
Liberando backups . . . 195
Eliminar backups . . . 196
Programación de backups de bases de datos . . . 198
Creando programaciones de backup . . . 198
Actualizar una programación de backup . . . 201
Ver una lista de operaciones programadas . . . 202
Suspensión de programaciones de backup . . . 202
Reanudar programaciones de backup . . . 202
Eliminación de programaciones de backup . . . 202
Restaurar backups de base de datos . . . 202
Qué es la restauración de base de datos . . . 203
Previsualizar la información de restauración de copias de seguridad . . . 226
Restauración de backups mediante restauración rápida . . . 228
Restauración de backups mediante Single File SnapRestore . . . 230
Restaurar backups en el almacenamiento principal . . . 230
Realizar recuperaciones a nivel de bloque con Oracle Recovery Manager (RMAN) . . . 235
Restaurar los archivos de una ubicación alternativa . . . 239
Clonar el backup de bases de datos . . . 244
Qué es la clonación . . . 244
Métodos de clonación . . . 246
Creando especificaciones de clon . . . 247
Clonar bases de datos a partir de backups . . . 254
Clonado de bases de datos en estado actual . . . 255
Clonado de backups de bases de datos sin necesidad de restablecer registros . . . 256
Consideraciones para clonar una base de datos en un host alternativo . . . 257
Ver una lista de clones . . . 258
Visualización de información detallada de los clones . . . 258

Eliminar clones . . . 259
Dividir un clon . . . 260
Introducción a la protección de datos en SnapManager . . . 263
¿Qué son las políticas de protección . . . 264
Qué estados de protección son . . . 265
Qué pools de recursos son . . . 265
Acerca de diferentes políticas de protección . . . 266
Configuración y habilitación de la protección de datos condicionada por políticas . . . 267
Cómo SnapManager retiene los backups en el almacenamiento local . . . 271
Aspectos que se deben tener en cuenta al realizar la protección de datos . . . 275
Protección de backups de bases de datos en almacenamiento secundario o terciario . . . 276
Restaurar backups protegidos a partir del almacenamiento secundario . . . 278
Clonar backups protegidos . . . 282
SnapManager para Oracle usa Protection Manager para proteger un backup de base de datos . . . 282
Detalles de la base de datos de destino . . . 283
Configuración y topología de almacenamiento principal y secundario . . . 283
Programa de backup y estrategia de retención . . . 287
Resumen de flujo de trabajo para backup de bases de datos local y secundario . . . 288
Protección de la configuración y ejecución de backups . . . 289
Restauración de base de datos desde backup . . . 298
Realizando operaciones de gestión . . . 300
Ver una lista de operaciones . . . 300
Ver los detalles de la operación . . . 300
Emitir comandos desde un host alternativo . . . 301
Comprobación de la versión del software SnapManager . . . 301
Detener el servidor host SnapManager . . . 301
Reiniciar el servidor host UNIX de SnapManager . . . 302
Desinstalar el software de un host UNIX . . . 302
Configuración de una notificación por correo electrónico . . . 302
Configuración de un servidor de correo para un repositorio . . . 304
Configuración de la notificación por correo electrónico para un perfil nuevo . . . 305
Configuración de la notificación por correo electrónico para un perfil existente . . . 307
Configuración de notificación por correo electrónico de resumen para varios perfiles . . . 308
Adición de un nuevo perfil para resumir las notificaciones por correo electrónico . . . 309
Adición de un perfil existente para resumir las notificaciones por correo electrónico . . . 309
Desactivar la notificación por correo electrónico para varios perfiles . . . 310
Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager . . . 310
Crear scripts de tareas previas, tareas posteriores y directivas . . . 312
Ver scripts de plugin de muestra . . . 324
Creación de scripts de tareas . . . 327
Almacenamiento de los scripts de tareas . . . 328
Verificar la instalación de los scripts de los plugins . . . 329
Creación de un archivo de especificación de tareas . . . 330
Realizar operaciones de backup, restauración y clonado mediante scripts previos y posteriores . . . 332

Actualizar el nombre del sistema de almacenamiento y el nombre de host de la base de datos de destino asociados con un perfil . . . 334
Actualizar el nombre del sistema de almacenamiento asociado con un perfil . . . 334
Ver una lista de sistemas de almacenamiento asociados a un perfil . . . 335
Actualizar el nombre de host de la base de datos de destino asociado a un perfil . . . 336
Mantener el historial de operaciones de SnapManager . . . 337
Configurar el historial de funcionamiento de SnapManager . . . 338
Ver una lista del historial de operaciones de SnapManager . . . 338
Ver el historial detallado de una operación específica asociada a un perfil . . . 339
Eliminando historial de operación de SnapManager . . . 339
Eliminar la configuración del historial asociada a un único perfil o a varios perfiles . . . 339
Ver detalles de configuración del historial de SnapManager . . . 339
Referencia de comandos de SnapManager para Oracle . . . 340
El comando smo_Server restart . . . 340
El comando start smo_Server . . . 341
El comando de estado del servidor smo_server . . . 341
El comando smo_Server stop . . . 342
El comando smo backup create . . . 343
El comando smo backup delete . . . 347
El comando libre de backup de smo . . . 348
El comando smo backup list . . . 350
El comando de montaje de backup de smo . . . 351
El comando smo backup restore . . . 353
El comando smo backup show . . . 358
El comando de desmontaje del backup de smo . . . 361
El comando de actualización de backup de smo . . . 362
El comando smo backup verify . . . 364
El comando smo clone create . . . 365
El comando smo clone delete . . . 369
El comando smo clone list . . . 370
El comando smo clone show . . . 371
El comando de plantilla de clon de smo . . . 374
El comando smo clone update . . . 375
El comando smo clone split-delete . . . 376
El comando smo clone split-estimation . . . 377
El comando de división de clones de smo . . . 378
El comando split-result de clon de smo . . . 384
El comando de parada por división de clones de smo . . . 385
El comando de estado dividido de clon de smo . . . 385
El comando smo clone detach . . . 386
El comando cmdfile de smo . . . 387
El comando smo credential clear . . . 388
El comando smo credential delete . . . 389
El comando smo credential list . . . 391
El comando smo credential set . . . 392

El comando smo history list . . . 394
El comando Operation-show de historial de smo . . . 395
El comando smo history purge . . . 396
El comando smo history remove . . . 397
El comando smo history set . . . 399
El comando smo history show . . . 400
El comando smo help . . . 401
El comando remove-summary-notification de la notificación de smo . . . 402
El comando de notificación de actualización-resumen-notificación de smo . . . 403
El comando smo notification set . . . 405
El comando de volcado de la operación de smo . . . 407
El comando smo operation list . . . 408
El comando smo operation show . . . 410
El comando smo password reset . . . 411
El comando smo plugin check . . . 412
El comando smo profile create . . . 413
El comando smo profile delete . . . 419
El comando smo profile destroy . . . 420
El comando smo profile dump . . . 421
El comando smo profile list . . . 421
El comando smo profile show . . . 423
El comando smo profile SYNC . . . 424
El comando smo profile update . . . 426
El comando smo profile verify . . . 432
El comando smo protection-policy . . . 433
El comando smo repository create . . . 434
El comando smo repository delete . . . 436
El comando rollback del almacén de smo . . . 438
El comando para actualizar el almacén de smo . . . 439
El comando smo repository show . . . 441
El comando de actualización del almacén de smo . . . 442
El comando smo schedule create . . . 444
El comando smo schedule delete . . . 449
El comando smo schedule list . . . 449
El comando smo schedule resume . . . 450
El comando smo schedule suspend . . . 450
El comando smo schedule update . . . 451
El comando smo Storage list . . . 452
El comando smo Storage rename . . . 453
El comando dump del sistema de smo . . . 454
El comando smo system verify . . . 454
El comando version de smo . . . 455
Resolución de problemas de SnapManager . . . 456
Volcar archivos . . . 462
Solucionar problemas de clones . . . 468

Solución de problemas de la interfaz gráfica de usuario . . . 471
Resolución de problemas de SnapDrive . . . 476
Solucionar problemas de cambio de nombre del sistema de almacenamiento . . . 478
Resolución de problemas conocidos . . . 479
Se produce un error en el montaje de un volumen FlexClone en un entorno NFS . . . 485
Se produce un error en la ejecución de varias operaciones paralelas en SnapManager . . . 485
No se puede restaurar la base de datos de RAC desde uno de los nodos de RAC donde no se creó el perfil . . . 486
Dónde obtener más información . . . 486
Clasificación de mensajes de error . . . 487
Mensajes de error . . . 489
Mensajes de error más comunes . . . 489
Mensajes de error asociados con el proceso de copia de seguridad de la base de datos (serie 2000) . . . 495
Errores de protección de datos . . . 497
Mensajes de error asociados con el proceso de restauración (serie 3000) . . . 501
Mensajes de error asociados con el proceso de clonación (serie 4000) . . . 503
Mensajes de error asociados con el proceso de gestión de perfiles (serie 5000) . . . 504
Mensajes de error asociados con la liberación de recursos de backup (series de backups 6000) . . . 504
Errores de interfaz de almacenamiento virtual (serie 8000 de interfaz de almacenamiento virtual) . . . 505
Mensajes de error asociados con el proceso de actualización gradual (serie 9000) . . . 505
Ejecución de operaciones (serie 12,000) . . . 506
Ejecución de componentes de proceso (serie 13,000) . . . 507
Mensajes de error asociados con utilidades de SnapManager (serie 14,000) . . . 508
Mensajes de error comunes de SnapDrive para UNIX . . . 509
Guía de instalación y administración . . . 511
Qué es para Oracle . . . 511
Qué hace SnapManager para Oracle . . . 511
Integración con otras aplicaciones y tecnologías de NetApp . . . 514
Ventajas de usar SnapManager . . . 515
En qué consiste la arquitectura de SnapManager para Oracle . . . 518
Qué repositorios son . . . 520
Qué perfiles son . . . 521
Qué son los estados de operación de SnapManager . . . 522
Cómo mantiene SnapManager la seguridad . . . 523
Acceso e impresión de la Ayuda en línea . . . 524
Consideraciones sobre la puesta en marcha de SnapManager para Oracle . . . 525
Requisitos para ejecutar SnapManager . . . 525
Compatibilidad con la versión de la base de datos y información general de la configuración . . . 527
Limitaciones al trabajar con SnapManager . . . 528
Las funciones de SnapManager y las tecnologías de Oracle no son compatibles con Windows . . . 532
Limitaciones de SnapManager para Clustered Data ONTAP . . . 533
Limitaciones relacionadas con Oracle Database . . . 533
Versiones obsoletas de la base de datos Oracle . . . 534
Instalar SnapManager para Oracle . . . 534
Preparar la instalación de SnapManager para Oracle . . . 534

Instalar SnapManager para Oracle . . . 536
Actualizar SnapManager . . . 537
Preparando la actualización de SnapManager . . . 537
Actualizar hosts SnapManager . . . 538
Tareas posteriores a la actualización . . . 539
Actualizar hosts de SnapManager mediante actualización gradual . . . 541
Configurando SnapManager . . . 548
Parámetros de configuración de SnapManager . . . 548
Comenzando por Oracle . . . 556
Identificación de una base de datos existente para realizar una copia de seguridad . . . 557
Verificación del estado del listener de Oracle . . . 557
Crear usuarios de Oracle para la base de datos del repositorio . . . 557
Crear un usuario de Oracle para la base de datos de destino . . . 558
Acceso a SnapManager . . . 558
Verificación del entorno . . . 561
Creación de repositorios . . . 562
Orden de realización de operaciones . . . 564
Seguridad y gestión de credenciales . . . 566
Qué es la autenticación de usuario . . . 566
Almacenamiento de contraseñas cifradas para secuencias de comandos personalizadas . . . 567
Autorizando el acceso al repositorio . . . 567
Autorizando el acceso a los perfiles . . . 568
Visualización de las credenciales de usuario . . . 568
Borrar credenciales de usuario para todos los hosts, repositorios y perfiles . . . 569
Eliminación de credenciales para recursos individuales . . . 570
Gestionar perfiles para backups eficientes . . . 570
Tareas relacionadas con perfiles . . . 571
Acerca de los perfiles y la autenticación . . . 571
Creación de perfiles . . . 571
Nomenclatura de copias Snapshot . . . 575
Cambiar el nombre de los perfiles . . . 577
Cambio de contraseñas de perfil . . . 578
Restablecimiento de la contraseña del perfil . . . 578
Autorizando el acceso a los perfiles . . . 579
Verificando perfiles . . . 579
Actualizando perfiles . . . 579
Eliminar perfiles . . . 583
Realizar backups de bases de datos . . . 583
Qué son los backups de la base de datos SnapManager . . . 584
Qué son los backups completos y parciales . . . 585
Acerca del manejo de archivos de registro de archivo y archivos de control . . . 591
Qué es la programación de backups de base de datos . . . 592
Creación de backups de la base de datos . . . 596
Qué es AutoSupport . . . 609
Verificación de los backups de las bases de datos . . . 610

Cambiar la política de retención de backups . . . 611
Ver una lista de backups . . . 612
Ver los detalles de backup . . . 613
Montar backups . . . 614
Desmontaje de backups . . . 614
Liberando backups . . . 615
Eliminar backups . . . 615
Programación de backups de bases de datos . . . 616
Creando programaciones de backup . . . 616
Actualizar una programación de backup . . . 619
Ver una lista de operaciones programadas . . . 620
Suspensión de programaciones de backup . . . 620
Reanudar programaciones de backup . . . 620
Eliminación de programaciones de backup . . . 620
Restaurar backups de base de datos . . . 620
Qué es la restauración de base de datos . . . 621
Previsualizar la información de restauración de copias de seguridad . . . 625
Restaurar backups en el almacenamiento principal . . . 626
Realizar recuperaciones a nivel de bloque con Oracle Recovery Manager (RMAN) . . . 630
Restaurar los archivos de una ubicación alternativa . . . 634
Clonar el backup de bases de datos . . . 637
Qué es la clonación . . . 637
Métodos de clonación . . . 639
Creando especificaciones de clon . . . 639
Clonar bases de datos a partir de backups . . . 646
Clonado de bases de datos en estado actual . . . 647
Clonado de backups de bases de datos sin necesidad de restablecer registros . . . 648
Consideraciones para clonar una base de datos en un host alternativo . . . 649
Ver una lista de clones . . . 650
Visualización de información detallada de los clones . . . 651
Eliminar clones . . . 651
Introducción a la protección de datos en SnapManager . . . 652
Cómo SnapManager retiene los backups en el almacenamiento local . . . 652
Aspectos que se deben tener en cuenta al realizar la protección de datos . . . 655
Protección de backups de bases de datos mediante scripts posteriores . . . 656
Realizando operaciones de gestión . . . 669
Ver una lista de operaciones . . . 669
Ver los detalles de la operación . . . 669
Emitir comandos desde un host alternativo . . . 670
Comprobación de la versión del software SnapManager . . . 670
Detener el servidor host SnapManager . . . 670
Reiniciar el servidor host SnapManager . . . 671
Desinstalando SnapManager . . . 671
Configuración de una notificación por correo electrónico . . . 671
Configuración de un servidor de correo para un repositorio . . . 673

Configuración de la notificación por correo electrónico para un perfil nuevo . . . 674
Configuración de la notificación por correo electrónico para un perfil existente . . . 676
Configuración de notificación por correo electrónico de resumen para varios perfiles . . . 677
Adición de un nuevo perfil para resumir las notificaciones por correo electrónico . . . 678
Adición de un perfil existente para resumir las notificaciones por correo electrónico . . . 678
Desactivar la notificación por correo electrónico para varios perfiles . . . 678
Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager . . . 679
Crear scripts de tareas previas, tareas posteriores y directivas . . . 681
Ver scripts de plugin de muestra . . . 692
Creación de scripts de tareas . . . 696
Almacenamiento de los scripts de tareas . . . 697
Verificar la instalación de los scripts de los plugins . . . 698
Creación de un archivo de especificación de tareas . . . 699
Realizar operaciones de backup, restauración y clonado mediante scripts previos y posteriores . . . 701
Actualizar el nombre del sistema de almacenamiento y el nombre de host de la base de datos de destino asociados con un perfil . . . 703
Actualizar el nombre del sistema de almacenamiento asociado con un perfil . . . 703
Ver una lista de sistemas de almacenamiento asociados a un perfil . . . 704
Actualizar el nombre de host de la base de datos de destino asociado a un perfil . . . 704
Mantener el historial de operaciones de SnapManager . . . 705
Configurar el historial de funcionamiento de SnapManager . . . 706
Ver una lista del historial de operaciones de SnapManager . . . 707
Ver el historial detallado de una operación específica asociada a un perfil . . . 707
Eliminando historial de operación de SnapManager . . . 707
Eliminar la configuración del historial asociada a un único perfil o a varios perfiles . . . 707
Ver detalles de configuración del historial de SnapManager . . . 707
Referencia de comandos de SnapManager para Oracle . . . 708
El comando smo_Server restart . . . 708
El comando start smo_Server . . . 709
El comando de estado del servidor smo_server . . . 709
El comando smo_Server stop . . . 710
El comando smo backup create . . . 711
El comando smo backup delete . . . 715
El comando libre de backup de smo . . . 716
El comando smo backup list . . . 717
El comando de montaje de backup de smo . . . 719
El comando smo backup restore . . . 721
El comando smo backup show . . . 724
El comando de desmontaje del backup de smo . . . 726
El comando de actualización de backup de smo . . . 728
El comando smo backup verify . . . 730
El comando smo clone create . . . 731
El comando smo clone delete . . . 734
El comando smo clone list . . . 736

El comando smo clone show . . . 737
El comando de plantilla de clon de smo . . . 738
El comando smo clone update . . . 739
El comando smo clone detach . . . 740
El comando cmdfile de smo . . . 741
El comando smo credential clear . . . 741
El comando smo credential delete . . . 742
El comando smo credential list . . . 744
El comando smo credential set . . . 745
El comando smo history list . . . 747
El comando Operation-show de historial de smo . . . 749
El comando smo history purge . . . 750
El comando smo history remove . . . 751
El comando smo history set . . . 752
El comando smo history show . . . 754
El comando smo help . . . 755
El comando remove-summary-notification de la notificación de smo . . . 756
El comando de notificación de actualización-resumen-notificación de smo . . . 757
El comando smo notification set . . . 758
El comando de volcado de la operación de smo . . . 760
El comando smo operation list . . . 761
El comando smo operation show . . . 763
El comando smo password reset . . . 764
El comando smo profile create . . . 765
El comando smo profile delete . . . 770
El comando smo profile dump . . . 771
El comando smo profile list . . . 771
El comando smo profile show . . . 773
El comando smo profile SYNC . . . 774
El comando smo profile update . . . 775
El comando smo profile verify . . . 780
El comando smo repository create . . . 782
El comando smo repository delete . . . 784
El comando rollback del almacén de smo . . . 786
El comando rollingupgrade del almacén de smo . . . 787
El comando smo repository show . . . 789
El comando de actualización del almacén de smo . . . 790
El comando smo schedule create . . . 792
El comando smo schedule delete . . . 796
El comando smo schedule list . . . 797
El comando smo schedule resume . . . 797
El comando smo schedule suspend . . . 798
El comando smo schedule update . . . 798
El comando smo Storage list . . . 800
El comando smo Storage rename . . . 800

El comando dump del sistema de smo . . . 801
El comando smo system verify . . . 802
El comando version de smo . . . 803
Resolución de problemas de SnapManager . . . 803
Volcar archivos . . . 811
Solucionar problemas de clones . . . 816
Solución de problemas de la interfaz gráfica de usuario . . . 818
Resolución de problemas conocidos . . . 823
Se produce un error en la ejecución de varias operaciones paralelas en SnapManager . . . 826
No se puede restaurar la base de datos de RAC desde uno de los nodos de RAC donde no se creó el perfil . . . 826
Dónde obtener más información . . . 827
Clasificación de mensajes de error . . . 828
Mensajes de error . . . 829
Mensajes de error más comunes . . . 830
Mensajes de error asociados con el proceso de copia de seguridad de la base de datos (serie 2000) . 834
Mensajes de error asociados con el proceso de restauración (serie 3000) . . . 836
Mensajes de error asociados con el proceso de clonación (serie 4000) . . . 837
Mensajes de error asociados con el proceso de gestión de perfiles (serie 5000) . . . 838
Mensajes de error asociados con la liberación de recursos de backup (series de backups 6000) . . . 838
Mensajes de error asociados con el proceso de actualización gradual (serie 9000) . . . 839
Ejecución de operaciones (serie 12,000) . . . 840
Ejecución de componentes de proceso (serie 13,000) . . . 840
Mensajes de error asociados con utilidades de SnapManager (serie 14,000) . . . 841
Avisos legales . . . 843
Derechos de autor . . . 843
Marcas comerciales . . . 843
Estadounidenses . . . 843
Política de privacidad . . . 843
Código abierto . . . 843

SnapManager 3.4.2 para Oracle

Bienvenido a la Biblioteca de información de SnapManager para Oracle. En este enlace encontrará información sobre SnapManager 3.4.2 para Oracle e incluye cómo configurar, gestionar y configurar el software para Clustered Data ONTAP y para Data ONTAP en 7-Mode.

Notas de la versión de SnapManager 3.4.2 para Oracle

La "Notas de la versión de SnapManager 3.4.2 para Oracle" describa las nuevas funciones, las notas de actualización, los problemas solucionados, las limitaciones conocidas y los problemas conocidos.

Debe iniciar sesión en el sitio de soporte de NetApp para acceder a las notas de la versión.

Guía de instalación y configuración para UNIX®

Esta guía describe las tareas iniciales que debe realizar para poner en marcha SnapManager 3.4.2 para Oracle con Clustered Data ONTAP en un entorno UNIX. Los temas incluyen cómo instalar y configurar el producto y cómo realizar una copia de seguridad de las bases de datos.

Información general del producto

SnapManager para Oracle automatiza y simplifica los procesos manuales asociados a operaciones como el backup, la recuperación y el clonado de bases de datos de Oracle, tareas de gran complejidad y que requieren mucho tiempo. Puede usar SnapManager con la tecnología SnapMirror de Data ONTAP para crear copias de backups en otro volumen, y también con la tecnología Data ONTAP SnapVault para archivar backups de forma eficiente a disco.

SnapManager se integra con tecnologías nativas de Oracle como Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) y Direct NFS en protocolos FC, iSCSI y NFS. De manera opcional, los backups creados mediante SnapManager se pueden catalogar con Oracle Recovery Manager (RMAN) para conservar la información de backups; estos backups se pueden utilizar posteriormente en operaciones de restauración a nivel de bloque o de recuperación a un momento específico de espacio de tabla.

Aspectos destacados de SnapManager

SnapManager integra perfectamente con las bases de datos Oracle en el host UNIX y es gracias a las tecnologías de copias Snapshot, SnapRestore y FlexClone de NetApp Ofrece una interfaz de usuario (UI) fácil de usar y una interfaz de línea de comandos (CLI) para funciones administrativas.

SnapManager permite realizar las siguientes operaciones de base de datos y gestionar los datos de forma eficiente:

- Creación de backups con gestión eficiente del espacio en almacenamiento primario o secundario

  SnapManager permite realizar backups de los archivos de datos y los archivos de registro de archivos por separado.

- Programación de backups
- Restauración de bases de datos completas o parciales mediante una operación de restauración basada en archivos o volúmenes
- Recuperación de bases de datos mediante la detección, el montaje y la aplicación de archivos de registro de archivos a partir de backups
- Eliminar archivos de registro de archivos de destinos de registro de archivos cuando se crean backups solo de los registros de archivos
- Si se conserva un número mínimo de backups de registros de archivos automáticamente, solo se deben retener los backups que contienen archivos únicos de registro de archivos
- Realizar un seguimiento de los detalles de las operaciones y generar informes
- Verificación de copias de seguridad para garantizar que las copias de seguridad tienen un formato de bloque válido y que ninguno de los archivos de copia de seguridad está dañado

- Mantener un historial de operaciones realizadas en el perfil de base de datos

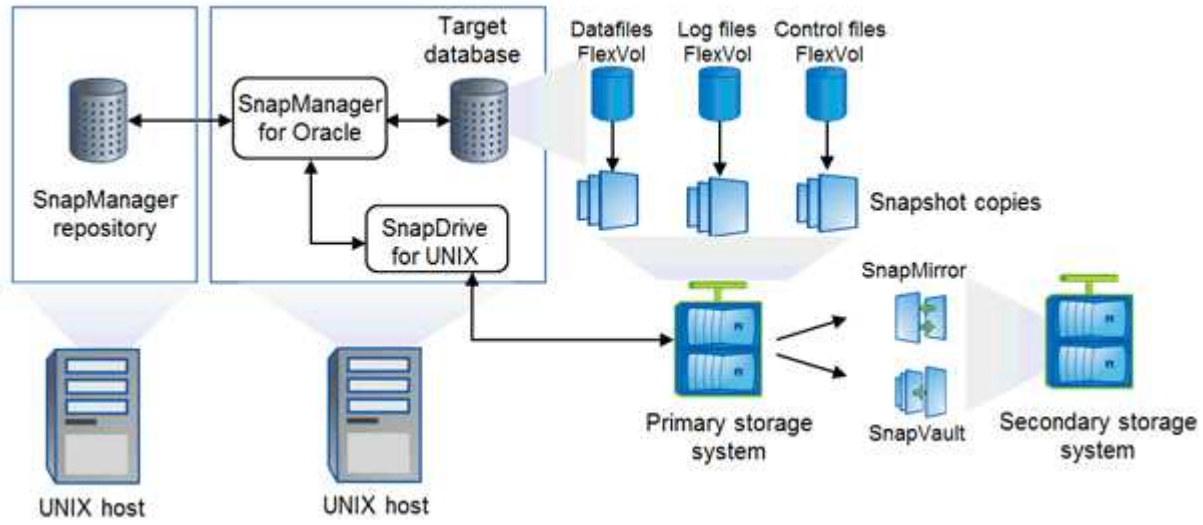
  Un perfil contiene información acerca de la base de datos que va a gestionar SnapManager.

- Proteger backups en sistemas de almacenamiento secundario
- Crear clones de backups con gestión eficiente del espacio en el almacenamiento principal o secundario

  SnapManager permite dividir el clon de una base de datos.

Arquitectura SnapManager

SnapManager para Oracle incluye componentes que trabajan conjuntamente para proporcionar una solución completa y potente de backup, restauración, recuperación y clonación para bases de datos Oracle.



SnapDrive para UNIX

SnapManager requiere que SnapDrive establezca la conexión con el sistema de almacenamiento. Debe instalar SnapDrive para UNIX en cada host de la base de datos de destino antes de instalar SnapManager.

SnapManager para Oracle

Debe instalar SnapManager para Oracle en cada host de la base de datos de destino.

Es posible usar la interfaz de línea de comandos (CLI) o la interfaz de usuario desde el host de base de datos donde se ha instalado SnapManager para Oracle. También puede usar la interfaz de usuario de SnapManager de forma remota mediante un explorador web desde cualquier sistema que se ejecute en un sistema operativo compatible con SnapManager.

Las versiones de JRE compatibles son 1.5, 1.6, 1.7 y 1.8.

Base de datos de destino

La base de datos de destino es una base de datos de Oracle que se desea gestionar mediante SnapManager para realizar operaciones de backup, restauración, recuperación y clonado.

La base de datos de destino puede ser independiente, Real Application Clusters (RAC) o residir en volúmenes de Oracle Automatic Storage Management (ASM). Para obtener detalles sobre las versiones, las configuraciones, los sistemas operativos y los protocolos de la base de datos de Oracle admitidos, consulte la herramienta de matriz de interoperabilidad de NetApp.

Repositorio de SnapManager

El repositorio de SnapManager reside en una base de datos de Oracle y almacena metadatos sobre perfiles, backups, restauración, recuperación y clonado. Un único repositorio puede contener información sobre las operaciones realizadas en varios perfiles de base de datos.

El repositorio de SnapManager no puede residir en la base de datos de destino. La base de datos del repositorio de SnapManager y la base de datos de destino deben estar en línea antes de ejecutar operaciones de SnapManager.

Sistema de almacenamiento primario

SnapManager realiza un backup de las bases de datos objetivo en el sistema de almacenamiento primario de NetApp.

Sistema de almacenamiento secundario

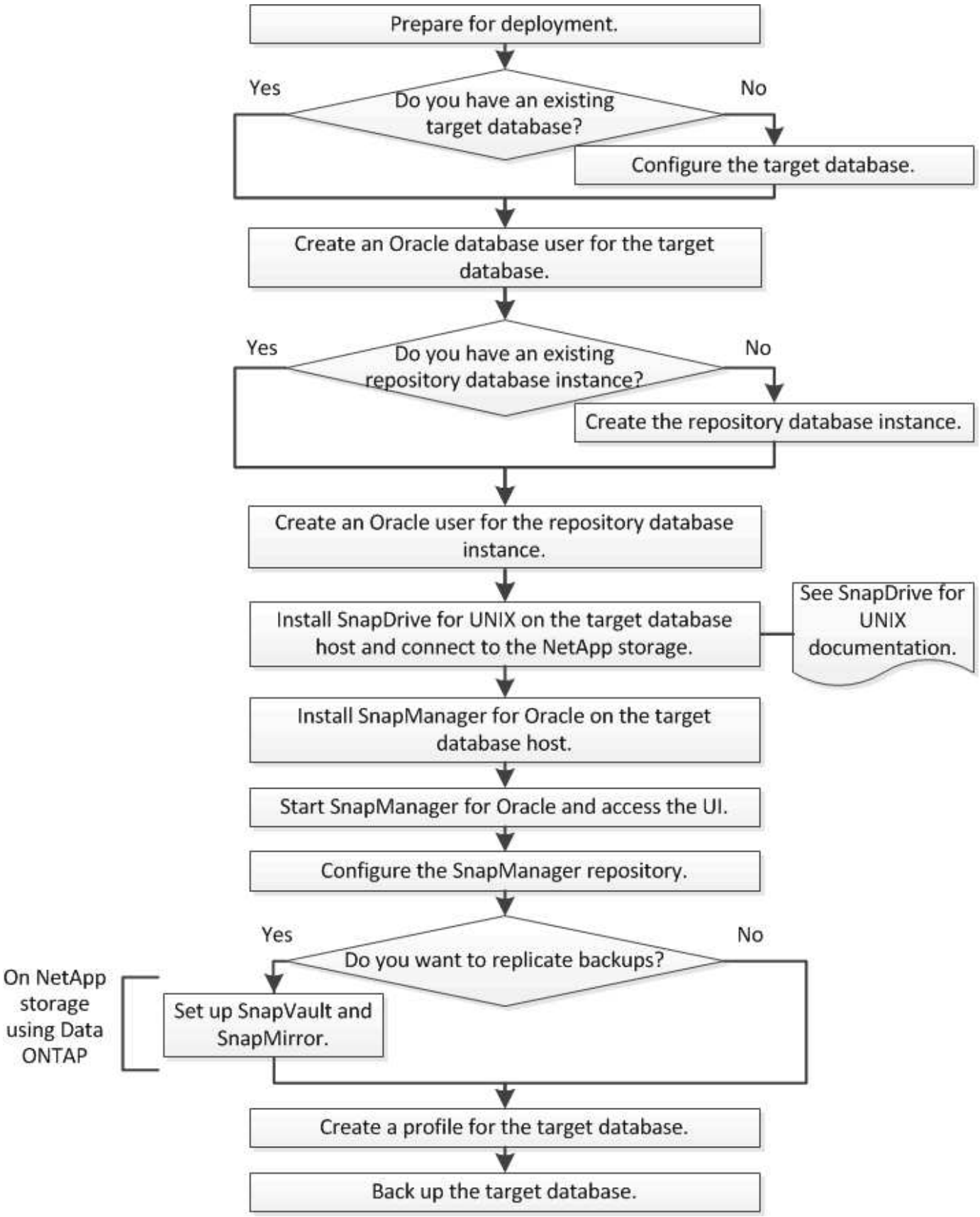
Cuando se habilita la protección de datos en un perfil de base de datos, los backups creados en el sistema de almacenamiento principal por SnapManager se replican en un sistema de almacenamiento secundario de NetApp mediante las tecnologías SnapVault y SnapMirror.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Flujo de trabajo de implementación

Antes de poder crear backups con SnapManager, primero debe instalar SnapDrive para UNIX y, a continuación, instalar SnapManager para Oracle.



Preparación para la implementación

Antes de implementar SnapManager, debe asegurarse de que el sistema de

almacenamiento y los hosts UNIX cumplen con los requisitos mínimos de recursos.

1. Compruebe que tiene las licencias necesarias.
2. Compruebe las configuraciones admitidas.
3. Compruebe los tipos de almacenamiento admitidos.
4. Verificar que los hosts UNIX cumplen los requisitos de SnapManager.

Licencias de SnapManager

Se requieren una licencia de SnapManager y varias licencias de sistema de almacenamiento para habilitar las operaciones de SnapManager. La licencia de SnapManager está disponible en dos modelos de licencia: Por servidor, en el que la licencia de SnapManager reside en cada host de bases de datos y en las licencias por sistema de almacenamiento, en las que la licencia de SnapManager reside en el sistema de almacenamiento.

Los requisitos de licencia de SnapManager son los siguientes:

Licencia	Descripción	Donde se la requiere
SnapManager por servidor	Una licencia del lado del host para un host de base de datos específico. Las licencias solo son obligatorias para los hosts de base de datos en los que está instalado SnapManager. No se requiere ninguna licencia de SnapManager para el sistema de almacenamiento.	En el host SnapManager. No se requiere una licencia de SnapManager en los sistemas de almacenamiento primarios y secundarios al usar la licencia por servidor.
SnapManager por sistema de almacenamiento	Una licencia del almacenamiento compatible con cualquier número de hosts de base de datos. Es obligatorio solo si no utiliza una licencia por servidor en el host de la base de datos.	En sistemas de almacenamiento principales y secundarios
SnapRestore	Una licencia requerida que permite a SnapManager restaurar bases de datos.	En sistemas de almacenamiento principal y secundario. Requerida en sistemas de destino de SnapMirror para realizar la verificación remota. Requerida en sistemas de destino de SnapVault para realizar la verificación remota y restaurar desde un backup

Licencia	Descripción	Donde se la requiere
FlexClone	Una licencia opcional para clonar bases de datos.	En sistemas de almacenamiento principal y secundario.requerida en sistemas de destino de SnapVault al crear clones a partir de un backup.
SnapMirror	Una licencia opcional para reflejar backups en un sistema de almacenamiento de destino.	En sistemas de almacenamiento principales y secundarios
SnapVault	Una licencia opcional para archivar backups en un sistema de almacenamiento de destino.	En sistemas de almacenamiento principales y secundarios
Protocolos	Se requieren licencias de NFS, iSCSI o FC en función del protocolo utilizado.	En sistemas de almacenamiento principales y secundarios Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible

Configuraciones admitidas

Los hosts en los que está instalando SnapManager deben cumplir con los requisitos especificados de software, explorador, base de datos y sistema operativo. Debe verificar la compatibilidad de la configuración antes de instalar o actualizar SnapManager.

Para obtener información sobre las configuraciones admitidas, consulte la herramienta de matriz de interoperabilidad.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Tipos de almacenamiento admitidos

SnapManager admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Es necesario verificar la compatibilidad de su tipo de almacenamiento antes de instalar o actualizar SnapManager.

Máquina	Tipo de almacenamiento
Servidor físico	• Volúmenes conectados en NFS • LUN conectados a FC • LUN conectados a iSCSI

Máquina	Tipo de almacenamiento
ESX de VMware	• Volúmenes NFS conectados directamente con el Guest VM • LUN de RDM en el sistema operativo invitado

Requisitos del host UNIX

Debe instalar SnapManager para Oracle en cada host donde esté alojada una base de datos de Oracle que desee realizar el backup. Debe asegurarse de que los hosts cumplan con los requisitos mínimos de la configuración de SnapManager.

- Debe instalar SnapDrive en el host de la base de datos antes de instalar SnapManager.
- Puede instalar SnapManager en equipos físicos o virtuales.
- Debe instalar la misma versión de SnapManager en todos los hosts que compartan el mismo repositorio.
- Debe instalar Oracle Patch 13366202 si utiliza bases de datos Oracle 11.2.0.2 o 11.2.0.3.

  Si utiliza DNFS, también debe instalar los parches enumerados en el informe de My Oracle Support (MOS) 1495104.1 para obtener el máximo rendimiento y estabilidad.

Configurar bases de datos

Debe configurar al menos dos bases de datos de Oracle: Una base de datos de destino para la que se desea realizar un backup con SnapManager y una base de datos de repositorio para almacenar los metadatos de la base de datos de destino. La base de datos de destino y la base de datos del repositorio de SnapManager deben estar configuradas y en línea antes de ejecutar operaciones de SnapManager.

Configurar la base de datos de destino

La base de datos de destino es una base de datos de Oracle que se puede configurar como independiente, Real Application Clusters (RAC), Automatic Storage Management (ASM) o cualquier otra combinación compatible.

1. Configure la base de datos de destino haciendo referencia a *TR-3633*.

Información relacionada

"Informe técnico de NetApp 3633: Mejores prácticas para las bases de datos de Oracle en el almacenamiento de NetApp"

Crear un usuario de base de datos de Oracle para la base de datos de destino

Se necesita un usuario de la base de datos de Oracle para iniciar sesión en la base de datos y ejecutar operaciones de SnapManager. Debe crear este usuario con el privilegio *sysdba* si no existe un usuario con el privilegio *sysdba* para la base de datos de destino.

SnapManager puede utilizar cualquier usuario de Oracle con el privilegio *sysdba* que existe para la base de datos de destino. Por ejemplo, SnapManager puede utilizar el usuario predeterminado *sys*. Sin embargo, incluso si el usuario existe, puede crear un nuevo usuario para la base de datos de destino y asignar el privilegio *sysdba*.

También puede usar el método de autenticación del SO en donde el sistema operativo (SO) permite que la base de datos Oracle utilice las credenciales que mantiene el sistema operativo para autenticar a los usuarios para iniciar sesión en la base de datos y ejecutar operaciones de SnapManager. Si el sistema operativo autentica, puede conectarse a la base de datos de Oracle sin especificar un nombre de usuario o una contraseña.

1. Iniciar sesión en SQL *Plus: Sqlplus '/ como sysdba'
2. Cree un nuevo usuario con una contraseña de administrador: Create useruser_name identificado por admin_password;

   user_name es el nombre de usuario que va a crear y admin_password es la contraseña que desea asignar al usuario.

3. Asigne el privilegio sysdba al nuevo usuario de Oracle: Conceda sysdba a nombre_usuario;

Crear la instancia de la base de datos del repositorio

La instancia de la base de datos del repositorio es una base de datos de Oracle en la que se crea el repositorio de SnapManager. La instancia de la base de datos del repositorio debe ser una base de datos independiente y no puede ser la base de datos de destino.

Debe tener una base de datos de Oracle y una cuenta de usuario para acceder a la base de datos.

1. Iniciar sesión en SQL *Plus: Sqlplus '/ como sysdba'
2. Cree un nuevo tablespace para el repositorio de SnapManager: Create tablespacetablenespace_name archivo de datos '/u01/app/oracle/oradata/archivo de datos/tablespace_name.dbf' size 100M autoexteNd activado;

   tablespace_name es el nombre del tablespace.

3. Verifique el tamaño de bloque del tablespace: Select tablespace_name, block_size from dba_tablespaces;

   SnapManager requiere un tamaño de bloque mínimo de 4 K para el espacio de tabla.

Información relacionada

"Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

Crear un usuario de Oracle para la instancia de la base de datos del repositorio

Se necesita un usuario de Oracle para iniciar sesión en la instancia de la base de datos del repositorio y acceder a ella. Debe crear este usuario con privilegios *connect* y *resource*.

1. Iniciar sesión en SQL *Plus: Sqlplus '/ como sysdba'

2. Cree un nuevo usuario y asigne una contraseña de administrador a ese usuario: Create useruser_name identificado por admin_password Default tablespace_name quota ilimitada en tablespace_name;
   - user_name es el nombre de usuario que va a crear para la base de datos del repositorio.
   - admin_password es la contraseña que desea asignar al usuario.
   - tablespace_name es el nombre del tablespace creado para la base de datos del repositorio.
3. Asigne los privilegios *connect* y *resource* al nuevo usuario de Oracle: Grant connect, resource to user_name;

Verificación de la configuración del listener de Oracle

El listener es un proceso que escucha las solicitudes de conexión de cliente. Recibe solicitudes entrantes de conexión de cliente y administra el tráfico de estas solicitudes a la base de datos. Antes de conectarse a una base de datos de destino o a una instancia de base de datos de repositorio, puede utilizar el comando STATUS para comprobar la configuración del listener.

El comando STATUS muestra información básica sobre el estado de un listener específico, incluyendo un resumen de la configuración del listener, las direcciones del protocolo de escucha y un resumen de los servicios registrados con ese listener.

1. Introduzca el siguiente comando en el símbolo del sistema: `lsnrctl STATUS`

   El valor predeterminado asignado al puerto de escucha es 1521.

Instalando SnapManager

Debe instalar SnapManager en cada host donde se ejecute la base de datos de la que desea realizar el backup.

Debe haber instalado SnapDrive para UNIX en el host de la base de datos y establecer una conexión con el sistema de almacenamiento.

Para obtener información sobre cómo instalar SnapDrive y establecer una conexión con el sistema de almacenamiento, consulte la documentación de SnapDrive para UNIX.

Debe instalar una instancia de SnapManager por cada host de bases de datos. Si usa una base de datos de RAC y desea realizar un backup de la base de datos de RAC, debe instalar SnapManager en todos los hosts de la base de datos de RAC.

1. Descargue el paquete de instalación de SnapManager para Oracle para UNIX desde el sitio de soporte de NetApp y cópielo al sistema host.

   "Descargas de NetApp: Software"

2. Inicie sesión en el host de la base de datos como usuario root.
3. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el paquete de instalación.
4. Haga ejecutable el paquete de instalación: Chmod 755install_package.bin
5. Instalar SnapManager: ./install_package.bin

6. Pulse Intro para continuar.
7. Siga estos pasos:
   a. Pulse Intro para aceptar el valor predeterminado del usuario del sistema operativo.

      el valor predeterminado para el usuario es oracle.

   b. Pulse Intro para aceptar el valor predeterminado para el grupo de sistemas operativos.

      El valor predeterminado para el grupo es dba.

   c. Pulse Intro para aceptar el valor predeterminado del tipo de inicio.

   Se muestra el resumen de la configuración.
8. Revise el resumen de la configuración y pulse Intro para continuar.

   SnapManager se instala en /opt/NTAPsmo para Solaris y en /opt/NetApp/ para todos los demás hosts UNIX.

Información relacionada

Configurar SnapManager

"Documentación de NetApp: SnapDrive para UNIX"

Configurar SnapManager

Puede iniciar SnapManager y acceder a ella mediante la interfaz de usuario (UI) o desde la interfaz de línea de comandos (CLI). Después de acceder a SnapManager, debe crear el repositorio de SnapManager antes de realizar cualquier operación de SnapManager.

Iniciando el servidor SnapManager

Debe iniciar el servidor SnapManager desde el host de la base de datos de destino.

1. Inicie sesión en el host de la base de datos de destino e inicie el servidor SnapManager: `smo_server start`

   Aparece el siguiente mensaje: Servidor SnapManager iniciado en puerto seguro Port_number con PID_Number.

   El puerto predeterminado es 27214.

Puede comprobar que SnapManager funciona correctamente: Verificación del sistema smo

Aparece el siguiente mensaje: Operación ID operation_ID_number succeeded.

Obtener acceso a la interfaz de usuario de SnapManager

Puede acceder a la interfaz de usuario de SnapManager de forma remota mediante un

explorador web desde cualquier sistema que se ejecute en un sistema operativo compatible con SnapManager. También puede acceder a la interfaz de usuario de SnapManager desde el host de la base de datos de destino ejecutando el comando smogui.

- Debe asegurarse de que SnapManager esté en ejecución.
- Debe asegurarse de que el sistema operativo y Java compatibles estén instalados en el sistema donde desea acceder a la interfaz de usuario de SnapManager.

  Para obtener información sobre el sistema operativo compatible y Java, consulte herramienta matriz de interoperabilidad.

  a. En la ventana del navegador web, introduzca lo siguiente:https://server_name.domain.com:port_number
     - Server_name es el nombre del host de la base de datos de destino donde está instalado SnapManager.

       También puede introducir la dirección IP del host de la base de datos de destino.
     - Port_number es el puerto en el que se ejecuta SnapManager.

       El valor predeterminado es 27214.

  b. Haga clic en el enlace **Iniciar SnapManager para Oracle**.

     Se mostrará la interfaz de usuario de SnapManager para Oracle.

Configurar el repositorio de SnapManager

Debe configurar el repositorio de SnapManager en la instancia de la base de datos del repositorio. La base de datos del repositorio almacena metadatos para las bases de datos gestionadas por SnapManager.

- Debe haber creado la instancia de la base de datos del repositorio.
- Debe haber creado el usuario de Oracle para la instancia de la base de datos del repositorio con los privilegios correspondientes.
- Debe haber incluido los detalles de la instancia de la base de datos del repositorio en el archivo tnsnames.ora.

Es posible configurar el repositorio de SnapManager desde la interfaz de usuario de SnapManager o desde la interfaz de línea de comandos (CLI). Estos pasos muestran cómo crear un repositorio con la interfaz de usuario de SnapManager. También puede utilizar la CLI si lo prefiere.

Para obtener información acerca de cómo crear el repositorio mediante la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el panel izquierdo de la interfaz de usuario de SnapManager, haga clic con el botón derecho del ratón en **repositorios**.
2. Seleccione **Crear nuevo repositorio** y haga clic en **Siguiente**.
3. En la ventana Repository Database Configuration Information (Información de configuración de la base de

datos del repositorio), introduzca la siguiente información:

En este campo…	Realice lo siguiente…
Nombre de usuario	Introduzca el nombre del usuario creado para la instancia de la base de datos del repositorio.
Contraseña	Introduzca la contraseña.
Host	Introduzca la dirección IP del host donde se crea la instancia de la base de datos del repositorio.
Puerto	Introduzca el puerto utilizado para conectarse a la instancia de la base de datos del repositorio. El puerto predeterminado es 1521.
Nombre del servicio	Introduzca el nombre que utiliza SnapManager para conectarse a la instancia de la base de datos del repositorio. Dependiendo de los detalles incluidos en el archivo tnsnames.ora, puede ser el nombre corto del servicio o el nombre completo del servicio. +

4. En la ventana realizar operación de adición del repositorio, revise el resumen de configuración y haga clic en **Agregar**.

   Si la operación falla, haga clic en la pestaña **Detalles de operación** para ver qué causó el error de la operación. Los detalles del error también se capturan en el registro de operaciones ubicado en /var/log/smo.

5. Haga clic en **Finalizar**.

   El repositorio aparece en el panel izquierdo bajo el árbol **repositorios**. Si no ve el repositorio, haga clic con el botón derecho del ratón en **repositorios** y haga clic en **Actualizar**.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault

Puede usar SnapManager con la tecnología SnapMirror de Data ONTAP para crear copias reflejadas de conjuntos de backups en otro volumen, y con la tecnología Data ONTAP SnapVault, para archivar backups de forma eficiente a disco. Para poder ejecutar estas tareas en SnapManager, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

No puede configurar una relación de SnapMirror y una relación de SnapVault en el mismo volumen de origen de Clustered Data ONTAP. Estas relaciones se deben configurar en volúmenes de origen diferentes.

Información relacionada

Comprender las diferencias entre SnapMirror y SnapVault

Preparar los sistemas de almacenamiento para la replicación de SnapMirror

Preparar sistemas de almacenamiento para la replicación de SnapVault

Comprender las diferencias entre SnapMirror y SnapVault

SnapMirror es la tecnología de recuperación ante desastres diseñada para la conmutación del almacenamiento principal al almacenamiento secundario en un sitio geográficamente remoto. SnapVault es una tecnología de archivado diseñada para la replicación de copias Snapshot disco a disco con el fin de cumplir los estándares y para otros fines relacionados con la regulación.

Estos objetivos tienen en cuenta el diferente equilibrio que ocurre cada tecnología entre los objetivos de la moneda de backup y la retención de backup:

- SnapMirror almacena *only* las copias Snapshot que residen en el almacenamiento principal porque, en caso de desastre, necesita poder realizar una conmutación al respaldo a la versión más reciente de los datos primarios que sabe que son buenos. Por ejemplo, la organización puede duplicar las copias de los datos de producción por hora en un plazo de diez días. Como se indica en el caso de uso de la conmutación por error, el equipo del sistema secundario debe ser equivalente o casi equivalente al equipo del sistema primario para servir datos de forma eficiente desde el almacenamiento duplicado.
- Por el contrario, SnapVault almacena las copias snapshot _independientemente de que residan en el almacenamiento principal porque, en caso de auditoría, es probable que el acceso a los datos históricos sea tan importante como el acceso a los datos actuales. Es posible que desee conservar copias Snapshot mensuales de sus datos en un período de 20 años (para cumplir, por ejemplo, las normativas de contabilidad gubernamental de su empresa). Como no hay necesidad de servir datos desde el almacenamiento secundario, puede utilizar discos más lentos y menos costosos en el sistema vault.

Por supuesto, los diferentes pesos de SnapMirror y SnapVault dan a las divisas de backup y la retención de backup se derivan en última instancia del límite de 255 copias de Snapshot en cada volumen. Donde SnapMirror conserva las copias más recientes, SnapVault conserva las copias realizadas durante el período de tiempo más largo.

Preparar los sistemas de almacenamiento para la replicación de SnapMirror

Antes de poder utilizar la tecnología SnapMirror integrada de SnapManager para reflejar copias Snapshot, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino; posteriormente, inicializar la relación. Tras la inicialización, SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot menos reciente del volumen de origen al volumen de destino.

- Debe crear los volúmenes de origen y destino en clústeres con una relación entre iguales con máquinas virtuales de almacenamiento (SVM). Para obtener más información, consulte la *Guía exprés* de relación de clústeres con clústeres de Clustered Data ONTAP.
- Debe ser un administrador de clústeres.
- Para la verificación de copias Snapshot en el volumen de destino, las SVM de origen y de destino deben tener una LIF de gestión y una LIF de datos. El LIF de gestión debe tener el mismo nombre DNS que la SVM. Defina la función de la LIF de gestión en los datos, el protocolo en none y la política de firewall en mgmt.

Puede usar la interfaz de línea de comandos (CLI) de Data ONTAP o System Manager de OnCommand para crear una relación de SnapMirror. El siguiente procedimiento asume que está utilizando la CLI. Para obtener información sobre la forma de crear relaciones de SnapMirror mediante System Manager de OnCommand, consulte la *Guía exprés de preparación para la recuperación de desastres de volúmenes de Clustered Data ONTAP*.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de SnapMirror:

1. Identifique el clúster de destino.
2. En el clúster de destino, use el comando volume create con la opción -typeDP para crear un volumen de destino de SnapMirror con un tamaño igual o mayor que el volumen de origen.

   La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

   El siguiente comando crea un volumen de destino de 2 GB denominado dstvolB en SVM2 en el agregado node01_aggr:

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

3. En la SVM de destino, utilice el comando snapmirror create con el parámetro -type DP para crear una relación de SnapMirror.

   El tipo de protección de datos define la relación como una relación de SnapMirror.

   El siguiente comando crea una relación de SnapMirror entre el volumen de origen srcvolA en SVM1 y el volumen de destino dstvolB en SVM2. De forma predeterminada, el comando asigna la política de SnapMirror predeterminada DPDefault:

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

   No defina una programación de mirroring para la relación de SnapMirror. SnapManager lo hace cuando se crea una programación de backup.

Si no desea utilizar la política predeterminada de SnapMirror, puede invocar el comando snapmirror policy create para definir una política de SnapMirror.

4. Utilice el comando snapmirror initialize para inicializar la relación.

   El proceso de inicialización realiza una transferencia básica al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot del volumen de origen al volumen de destino.

   El siguiente comando inicializa la relación entre el volumen de origen srcvolA en SVM1 y el volumen de destino dstvolB en SVM2:

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

Información relacionada

"Guía exprés de relación de clústeres entre iguales de Clustered Data ONTAP 8.3"

"Guía exprés de preparación para la recuperación de desastres de volúmenes de Clustered Data ONTAP 8.3"

Preparar sistemas de almacenamiento para la replicación de SnapVault

Antes de poder utilizar la tecnología SnapVault integrada de SnapManager para archivar copias Snapshot en disco, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino; a continuación, inicializar la relación. Durante la inicialización, SnapVault realiza una copia Snapshot del volumen de origen, a continuación transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino.

- Debe crear los volúmenes de origen y destino en clústeres con una relación entre iguales con máquinas virtuales de almacenamiento (SVM). Para obtener más información, consulte la *Guía exprés* de relación de clústeres con clústeres de Clustered Data ONTAP.
- Debe ser un administrador de clústeres.

Puede usar la interfaz de línea de comandos (CLI) de Data ONTAP o System Manager de OnCommand para crear relaciones de SnapVault. El siguiente procedimiento asume que está utilizando la CLI. Para obtener información acerca de cómo crear relaciones de SnapVault mediante System Manager de OnCommand, consulte la *Guía exprés* de backup de volúmenes de Data ONTAP en clúster mediante SnapVault.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de SnapVault:

1. Identifique el clúster de destino.
2. En el clúster de destino, use el comando volume create con la opción -typeDP para crear un volumen de destino de SnapVault con el mismo tamaño o más que el volumen de origen.

   La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

El siguiente comando crea un volumen de destino de 2 GB denominado dstvolB en SVM2 en el agregado node01_aggr:

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

3. En la SVM de destino, utilice el comando snapmirror policy create para crear una política de SnapVault.

   El siguiente comando crea la política SVM1-vault para toda la SVM:

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

> No defina una programación de cron o una política de copia de Snapshot para la relación de SnapVault. SnapManager lo hace cuando se crea una programación de backup.

4. Utilice el comando SnapMirror policy add-rule para añadir una regla a la política que define las siguientes etiquetas de copia de Snapshot y la política de retención de cada etiqueta:
   - Todos los días
   - Semanal
   - Mensual
   - Cada hora
   - Ilimitado **importante:** las etiquetas son sensibles a las mayúsculas y minúsculas.

     Se trata de etiquetas fijas que utiliza SnapManager. Al archivar una copia de seguridad, seleccione una de estas opciones. Debe ejecutar este comando una vez para cada una de las reglas que va a agregar.

     + el siguiente comando agrega una regla a la política de almacén SVM1 que define la etiqueta "día" y especifica que se deben conservar en el almacén treinta copias Snapshot que coincidan con la etiqueta:

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

1. Utilice el comando snapmirror create con el parámetro -type XDP y el parámetro -policy para crear una relación de SnapVault y asignar una política de almacén.

   El tipo XDP define la relación como una relación de SnapVault.

   El siguiente comando crea una relación de SnapVault entre el volumen de origen srcvolA en SVM1 y el volumen de destino dstvolB en SVM2. Asigna la directiva denominada SVM1-vault:

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

2. Utilice el comando snapmirror initialize para inicializar la relación.

   El proceso de inicialización realiza una transferencia básica al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino.

   El siguiente comando inicializa la relación entre el volumen de origen srcvolA en SVM1 y el volumen de destino dstvolB en SVM2:

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

Información relacionada

"Guía exprés de relación de clústeres entre iguales de Clustered Data ONTAP 8.3"

"Guía exprés de backup de volúmenes mediante SnapVault de Clustered Data ONTAP 8.3"

Realizar backup y verificación de las bases de datos

Después de instalar SnapManager, puede crear una copia de seguridad básica de la base de datos y comprobar que la copia de seguridad no contiene ningún archivo dañado.

Información relacionada

Información general sobre backup de SnapManager

Definición de una estrategia de backup

Crear un perfil para la base de datos

Realizar una copia de seguridad de la base de datos

Verificación de los backups de las bases de datos

Programación de copias de seguridad periódicas

Información general sobre backup de SnapManager

SnapManager utiliza la tecnología Snapshot de NetApp para crear backups de bases de datos. Puede utilizar la utilidad DBVERIFY o SnapManager para verificar la integridad de las copias de seguridad.

SnapManager realiza un backup de una base de datos mediante la creación de copias Snapshot de los volúmenes que contienen archivos de datos, archivos de control y archivos de registro de archivos. Juntas,

estas copias Snapshot incluyen un conjunto de respaldos que SnapManager puede usar para restaurar una base de datos.

Definición de una estrategia de backup

Definir una estrategia de backup antes de crear backups garantiza que se cuente con todos los backups para restaurar correctamente las bases de datos. SnapManager ofrece un programa de backup granular y flexible para cumplir con el acuerdo de nivel de servicio.

> Para obtener información sobre las prácticas recomendadas de SnapManager, consulte *TR 3761*.

¿Qué modo de backup de SnapManager necesita?

SnapManager admite dos modos de backup:

Modo de backup	Descripción
Backup en línea	Crea un backup de la base de datos cuando la base de datos está en estado en línea. Este modo de backup también se denomina backup dinámico.
Backup sin conexión	Crea un backup de la base de datos cuando la base de datos está en estado montado o apagado. Este modo de backup también se denomina backup en frío.

¿Qué tipo de backup de SnapManager necesita?

SnapManager admite tres tipos de backups:

Tipo de backup	Descripción
Backup completo	Crea un backup de la base de datos completa, que incluye todos los archivos de datos, los archivos de control y los archivos de registro de archivos.
Copia de seguridad parcial	Crea un backup de archivos de datos, archivos de control, espacios de tabla y archivos de registro de archivos seleccionados
Backup de solo registro de archivo	Crea una copia de seguridad sólo de los archivos de registro de archivo.debe seleccionar **copia de seguridad de archivos por separado** mientras crea el perfil.

¿Qué tipo de perfil de base de datos necesita?

SnapManager crea backups según si el perfil de la base de datos separa los backups de los registros de archivo de los backups del archivo de datos.

Tipo de perfil	Descripción
Un único perfil de base de datos para el backup combinado de archivos de datos y registros de archivos	Permite crear: • Backup completo que contiene todos los archivos de datos, los archivos de registro del archivo y los archivos de control • Backup parcial con los archivos de datos, espacios de tabla, archivos de registro de archivo y archivos de control seleccionados
Perfiles de base de datos separados para backups de registros de archivo y backups de archivos de datos	Permite crear: • Backup combinado con distintas etiquetas para backup de archivos de datos y backup de registros de archivo • Backup de solo archivos de datos de todos los archivos de datos junto con los archivos de control • Backup parcial de solo archivos de datos de los archivos de datos o espacios de tablas seleccionados junto con los archivos de control • Backup de solo registros de archivo

¿Qué convenciones de nomenclatura se deben utilizar para las copias Snapshot?

Las copias Snapshot creadas por los backups pueden seguir una convención de nomenclatura personalizada. El texto personalizado o las variables integradas, como el nombre del perfil, el nombre de la base de datos y el SID de la base de datos proporcionado por SnapManager, se pueden utilizar para crear la convención de nomenclatura. Puede crear la convención de nomenclatura mientras crea la política.

> Debe incluir la variable smid en el formato de nomenclatura. La variable smid crea un identificador de instantánea único.

La convención de nomenclatura de las copias Snapshot se puede cambiar durante o después de la creación de un perfil. El patrón actualizado se aplica solo a las copias Snapshot que todavía no se han creado; las copias Snapshot existentes conservan el patrón anterior.

¿Cuánto tiempo desea retener las copias de backup en el sistema de almacenamiento primario y en el sistema de almacenamiento secundario?

Una política de retención de backup especifica la cantidad de backups correctos que se retendrán. Puede especificar la política de retención mientras crea la política.

Puede seleccionar cada hora, día, semana, mensual o ilimitado como clase de retención. Para cada clase de retención, puede especificar el recuento de retención y la duración de la retención, ya sea de forma conjunta o

individual.

- El recuento de retenciones determina la cantidad mínima de backups de una clase de retención determinada que se deben retener.

  Por ejemplo, si la programación de backup es *Daily* y el recuento de retenciones es *10*, se conservan 10 backups diarios.

  > El número máximo de copias de Snapshot que Data ONTAP permite retener es de 255. Cuando alcance el límite máximo, se producirá un error al crear nuevas copias Snapshot de forma predeterminada. Sin embargo, puede configurar la política de rotación en Data ONTAP para eliminar copias Snapshot más antiguas.

- La duración de la retención determina la cantidad mínima de días durante los cuales se debe conservar el backup.

  Por ejemplo, si la programación de la copia de seguridad es *Daily* y la duración de la retención es *10*, se retienen 10 días de los backups diarios.

Si se configura la replicación de SnapMirror, la política de retención se refleja en el volumen de destino.

> Para la retención a largo plazo de copias de backup, es conveniente usar SnapVault.

¿Desea verificar las copias de backup con el volumen de origen o un volumen de destino?

Si usa SnapMirror o SnapVault, puede verificar las copias de backups con la copia de Snapshot en el volumen de destino de SnapMirror o SnapVault, en lugar de la copia de Snapshot en el sistema de almacenamiento principal. Al utilizar un volumen de destino para verificar, se reduce la carga para el sistema de almacenamiento principal.

Información relacionada

"Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

Crear un perfil para la base de datos

Debe crear un perfil para que la base de datos pueda realizar cualquier operación en esa base de datos. El perfil contiene información acerca de la base de datos y sólo puede hacer referencia a una base de datos; sin embargo, varios perfiles pueden hacer referencia a una base de datos. No es posible acceder a una copia de seguridad creada con un perfil desde otro perfil, incluso si ambos perfiles están asociados con la misma base de datos.

Asegúrese de que los detalles de la base de datos objetivo se incluyan en el archivo /etc/oratab.

Estos pasos muestran cómo crear un perfil para la base de datos con la interfaz de usuario de SnapManager. También puede utilizar la CLI si lo prefiere.

Para obtener información acerca de cómo crear perfiles mediante la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el árbol repositorios, haga clic con el botón secundario del ratón en el repositorio o en el host y

seleccione **Crear perfil**.

2. En la página Información de configuración del perfil, introduzca el nombre y la contraseña personalizados del perfil.
3. En la página Database Configuration Information, introduzca la siguiente información:

En este campo…	Realice lo siguiente…
Nombre de la base de datos	Introduzca el nombre de la base de datos de la que desea realizar backup.
SID de base de datos	Introduzca el ID seguro (SID) de la base de datos. El nombre de la base de datos y el SID de la base de datos pueden ser iguales.
Host	Introduzca la dirección IP del host en el que reside la base de datos de destino. También puede especificar el nombre de host si el nombre de host se especifica en el sistema de nombres de dominio (DNS).
Cuenta de host	Introduzca el nombre de usuario de Oracle de la base de datos de destino. el valor predeterminado para el usuario es oracle.
Grupo de hosts	Introduzca el nombre del grupo de usuarios de Oracle. El valor predeterminado es dba. +

4. En la página Database Connection Information, seleccione una de las siguientes opciones:

Elija esto…	Si desea…
Usar autenticación de o/S	Utilice las credenciales que mantiene el sistema operativo para autenticar a los usuarios que acceden a la base de datos.

Usar autenticación de base de datos	Permitir que Oracle autentique un usuario administrativo mediante la autenticación del archivo de contraseña. Introduzca la información de conexión de la base de datos adecuada. • En el campo **SYSDBA Privileged User Name**, introduzca el nombre del administrador de la base de datos con privilegios administrativos. • En el campo **Contraseña**, introduzca la contraseña del administrador de la base de datos. • En el campo **Puerto**, introduzca el número de puerto utilizado para conectarse al host en el que reside la base de datos. El valor predeterminado es 1521.
Usar autenticación de instancia de ASM	Permitir que la instancia de la base de datos de Automatic Storage Management (ASM) autentique un usuario administrativo. Introduzca la información de autenticación de la instancia de ASM correspondiente. • En el campo **SYSDBA/SYSASM Privileged User Name**, introduzca el nombre de usuario del administrador de la instancia de ASM con privilegios administrativos. • En el campo **Contraseña**, introduzca la contraseña del administrador.

Nota: sólo puede seleccionar el modo de autenticación ASM si tiene una instancia ASM en el host de la base de datos.

5. En la página Información de configuración de RMAN, seleccione una de las siguientes opciones:

Elija esto…	Si…
No utilice RMAN	No se utiliza RMAN para gestionar las operaciones de backup y restauración.
Usar RMAN a través del archivo de control	Se gestiona el repositorio de RMAN mediante archivos de control.

Usar RMAN a través del Catálogo de recuperación	Se gestiona el repositorio de RMAN mediante la base de datos de catálogo de recuperación. Introduzca el nombre de usuario que tiene acceso a la base de datos del catálogo de recuperación, la contraseña y el nombre del servicio de red de Oracle de la base de datos que gestiona la conexión de sustrato de red transparente (TNS). +

6. En la página Snapshot Naming Information, seleccione las variables para especificar un formato de nomenclatura para la copia Snapshot.

   Debe incluir la variable smid en el formato de nomenclatura. La variable smid crea un identificador de instantánea único.

7. En la página Policy Settings, realice lo siguiente:
   a. Introduzca el recuento y la duración de la retención para cada clase de retención.
   b. En la lista desplegable **Política de protección**, seleccione la política de protección.

      Debe seleccionar las políticas de *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault* en función de si se ha establecido una relación de SnapMirror o SnapVault.

   c. Si desea realizar una copia de seguridad de los registros de archivos por separado, active la casilla de verificación **copia de seguridad de archivos por separado**, especifique la retención y seleccione la política de protección.

      Puede seleccionar una política que sea diferente de la asociada para los archivos de datos. Por ejemplo, si ha seleccionado *SnapManager_CDOT_Mirror* para archivos de datos, puede seleccionar *SnapManager_CDOT_Vault* para los registros de archivos.

8. En la página Configure Notification Settings, especifique los ajustes de notificación por correo electrónico.
9. En la página Información de configuración del historial, seleccione una de las opciones para mantener el historial de operaciones de SnapManager.
10. En la página Perform Profile Create Operation, compruebe la información y haga clic en **Crear**.
11. Haga clic en **Finalizar** para cerrar el asistente.

    Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Realizar una copia de seguridad de la base de datos

Después de crear un perfil, debe realizar un backup de la base de datos. Se pueden programar backups recurrentes después del backup y la verificación iniciales.

Estos pasos muestran cómo crear un backup de la base de datos con la interfaz de usuario de SnapManager. También puede usar la interfaz de línea de comandos (CLI) si lo prefiere.

Para obtener información acerca de cómo crear copias de seguridad mediante la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el árbol repositorios, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos de la que desea realizar la copia de seguridad y seleccione **copia de seguridad**.
2. En **Label**, introduzca un nombre personalizado para la copia de seguridad.

   No debe incluir espacios ni caracteres especiales en el nombre. Si no se especifica un nombre, SnapManager crea automáticamente una etiqueta de backup.

   En SnapManager 3.4, es posible modificar la etiqueta de backup creada automáticamente por SnapManager. Puede editar las variables de configuración override.default.backup.pattern y new.default.backup.pattern para crear su propio patrón de etiqueta de copia de seguridad predeterminado.

3. En **etiqueta de SnapVault**, debe introducir la etiqueta de SnapMirror que ha especificado en las reglas de la política de SnapMirror al configurar la relación de SnapVault.

   > El campo **etiqueta de SnapVault** sólo aparece si ha seleccionado *SnapManager_CDOT_Vault* como política de protección al crear el perfil.

4. Seleccione **permitir inicio o cierre de la base de datos, si es necesario** para modificar el estado de la base de datos, si es necesario.

   Esta opción garantiza que si la base de datos no está en el estado requerido para crear un backup, SnapManager automáticamente llevará la base de datos al estado deseado a fin de completar la operación.

5. En la página Database, Tablespaces o Datafiles to Backup, realice lo siguiente:
   a. Seleccione **copia de seguridad de archivos de datos** para realizar una copia de seguridad de la base de datos completa, los archivos de datos seleccionados o los tablespaces seleccionados.
   b. Seleccione **copia de seguridad Archivelogs** para realizar una copia de seguridad de los archivos de registro de archivos por separado.
   c. Seleccione **Prune Archivelogs** si desea eliminar los archivos de registro de archivos del sistema de archivos activo del que ya se ha realizado una copia de seguridad.

      > Si está habilitado el área de recuperación de flash (FRA) para los archivos de registro de archivos, SnapManager no puede depurar los archivos de registro de archivos.

   d. Seleccione **proteger la copia de seguridad** si desea activar la protección de copia de seguridad.

      Esta opción sólo está activada si se ha seleccionado la directiva de protección al crear el perfil.

   e. En la lista desplegable **Tipo**, seleccione el tipo de copia de seguridad (sin conexión o en línea) que desea crear.

      Si selecciona Auto, SnapManager crea un backup según el estado actual de la base de datos.

   f. En la lista desplegable **clase de retención**, seleccione la clase de retención.
   g. Active la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** si desea asegurarse de que los archivos de copia de seguridad no están dañados.
6. En la página Task Enabling, especifique si desea realizar tareas antes y después de que se completen las

operaciones de backup.

7. En la página realizar operaciones de copia de seguridad, compruebe la información y haga clic en **copia de seguridad**.
8. Haga clic en **Finalizar** para cerrar el asistente.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Verificación de los backups de las bases de datos

Puede verificar la copia de seguridad de la base de datos para asegurarse de que los archivos de los que se ha realizado una copia de seguridad no estén dañados.

Si no ha seleccionado la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** al crear una copia de seguridad, debe realizar estos pasos manualmente para verificar la copia de seguridad. Sin embargo, si seleccionó esta casilla de comprobación, SnapManager verifica automáticamente el backup.

1. En el árbol **repositorios**, seleccione el perfil.
2. Haga clic con el botón derecho del ratón en la copia de seguridad que desee verificar y seleccione **verificar**.
3. Haga clic en **Finalizar**.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

   En el árbol **repositorio**, haga clic con el botón secundario del ratón en la copia de seguridad y, a continuación, haga clic en **Propiedades** para ver los resultados de la operación de verificación.

Es posible usar archivos de backup para realizar operaciones de restauración. Para obtener información acerca de cómo realizar operaciones de restauración con la interfaz de usuario de SnapManager, consulte *Ayuda en línea*. Si desea utilizar la interfaz de línea de comandos (CLI) para realizar operaciones de restauración, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Programación de copias de seguridad periódicas

Es posible programar operaciones de backup para que los backups se inicien automáticamente a intervalos regulares. SnapManager permite programar backups por hora, día, semana, mes o una sola vez.

Es posible asignar varias programaciones de backup para una sola base de datos. Sin embargo, cuando se programen varios backups para la misma base de datos, se debe asegurarse de que no se hayan programado al mismo tiempo.

Estos pasos muestran cómo crear una programación de backups para la base de datos con la interfaz de

usuario de SnapManager. También puede usar la interfaz de línea de comandos (CLI) si lo prefiere. Para obtener información acerca de cómo programar copias de seguridad utilizando la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el árbol repositorios, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos para la que desea crear una programación de copia de seguridad y seleccione **copia de seguridad programada**.
2. En **Label**, introduzca un nombre personalizado para la copia de seguridad.

   No debe incluir espacios ni caracteres especiales en el nombre. Si no se especifica un nombre, SnapManager crea automáticamente una etiqueta de backup.

   En SnapManager 3.4, es posible modificar la etiqueta de backup creada automáticamente por SnapManager. Puede editar las variables override.default.backup.pattern y new.default.backup.patternconfiguration para crear su propio patrón de etiqueta de copia de seguridad predeterminado.

3. En **etiqueta de SnapVault**, debe introducir la etiqueta de SnapMirror que ha especificado en las reglas de la política de SnapMirror al configurar la relación de SnapVault.

   > El campo **etiqueta de SnapVault** sólo aparece si ha seleccionado *SnapManager_CDOT_Vault* como política de protección al crear el perfil.

4. Seleccione **permitir inicio o cierre de la base de datos, si es necesario** para modificar el estado de la base de datos, si es necesario.

   Esta opción garantiza que si la base de datos no está en el estado requerido para crear un backup, SnapManager automáticamente llevará la base de datos al estado deseado a fin de completar la operación.

5. En la página Database, Tablespaces o Datafiles to Backup, realice lo siguiente:
   a. Seleccione **copia de seguridad de archivos de datos** para realizar una copia de seguridad de la base de datos completa, los archivos de datos seleccionados o los tablespaces seleccionados.
   b. Seleccione **copia de seguridad Archivelogs** para realizar una copia de seguridad de los archivos de registro de archivos por separado.
   c. Seleccione **Prune Archivelogs** si desea eliminar los archivos de registro de archivos del sistema de archivos activo del que ya se ha realizado una copia de seguridad.

      > Si está habilitado el área de recuperación de flash (FRA) para los archivos de registro de archivos, SnapManager no puede depurar los archivos de registro de archivos.

   d. Seleccione **proteger la copia de seguridad** si desea activar la protección de copia de seguridad.

      Esta opción sólo está activada si se ha seleccionado la directiva de protección al crear el perfil.

   e. En la lista desplegable **Tipo**, seleccione el tipo de copia de seguridad (sin conexión o en línea) que desea crear.

      Si selecciona Auto, SnapManager crea un backup según el estado actual de la base de datos.

   f. En la lista desplegable **clase de retención**, seleccione la clase de retención.
   g. Active la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** si

desea asegurarse de que los archivos de copia de seguridad no están dañados.

6. En el campo **Nombre de programa**, introduzca un nombre personalizado de la programación.

   No debe incluir espacios en el nombre.

7. En la página Configure Backup Schedule, realice lo siguiente:
   a. En la lista desplegable **Perform this operation**, seleccione la frecuencia de la programación de copia de seguridad.
   b. En el campo **Fecha de inicio**, especifique la fecha en la que desea iniciar el programa de copia de seguridad.
   c. En el campo **Hora de inicio**, especifique la hora a la que desea iniciar el programa de copia de seguridad.
   d. Especifique el intervalo en el que se crearán los backups.

      Por ejemplo, si ha seleccionado la frecuencia por hora y especifica el intervalo como 2, los backups se programarán cada 2 horas.

8. En la página Task Enabling, especifique si desea realizar tareas antes y después de que se completen las operaciones de backup.
9. En la página realizar operación de programación de copia de seguridad, compruebe la información y haga clic en **Programación**.
10. Haga clic en **Finalizar** para cerrar el asistente.

    Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

A continuación, ¿dónde ir

Después de instalar SnapManager y crear correctamente un backup, puede utilizar SnapManager para realizar operaciones de restauración, recuperación y clonado. Además, se recomienda buscar información sobre otras funciones de SnapManager, como la programación, la gestión de operaciones de SnapManager y el mantenimiento del historial de operaciones.

Es posible encontrar más información sobre estas funciones, así como información específica de la versión de SnapManager, en la siguiente documentación, toda la cual está disponible en "Soporte de NetApp".

- "Guía de administración para UNIX de SnapManager 3.4 para Oracle"

  Describe cómo configurar y administrar SnapManager para Oracle. Los temas incluyen cómo configurar, realizar backup, restaurar y clonar bases de datos, realizar una protección secundaria, Además, una explicación de los comandos de la CLI e instrucciones sobre cómo actualizar y desinstalar el producto.

- "Notas de la versión de SnapManager 3.4 para Oracle"

  Describe nuevas funciones, problemas solucionados, precauciones importantes, problemas conocidos y limitaciones de SnapManager para Oracle.

- *Ayuda en línea de SnapManager para Oracle*

  Describe los procedimientos paso a paso para realizar diferentes operaciones de SnapManager mediante la interfaz de usuario de SnapManager.

  > El *Ayuda en línea* se integra con la interfaz de usuario de SnapManager y no está disponible en el sitio de soporte.

- "Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

  Describe las prácticas recomendadas de SnapManager para Oracle.

- "Informe técnico de NetApp 3633: Mejores prácticas para las bases de datos de Oracle en el almacenamiento de NetApp"

  Describe las prácticas recomendadas para configurar las bases de datos de Oracle en el sistema de almacenamiento de NetApp.

Información relacionada

"Soporte de NetApp"

"Documentación de NetApp: Biblioteca de productos A-Z"

Guía de instalación y configuración para UNIX®

Esta guía indica las tareas iniciales que debe realizar para implementar SnapManager 3.4.2 para Oracle con Data ONTAP funcionando en 7-Mode en un entorno UNIX. Los temas incluyen cómo instalar y configurar el producto y cómo realizar una copia de seguridad de las bases de datos.

Información general del producto

Automatiza y simplifica los procesos manuales asociados a operaciones como el backup, la recuperación y el clonado de bases de datos de Oracle, tareas de gran complejidad y que requieren mucho tiempo. Puede usar SnapManager con la tecnología SnapMirror de Data ONTAP para crear copias de backups en otro volumen, y también con la tecnología Data ONTAP SnapVault para archivar backups de forma eficiente a disco.

SnapManager se integra con tecnologías nativas de Oracle como Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) y Direct NFS en protocolos FC, iSCSI y NFS. De manera opcional, los backups creados mediante SnapManager se pueden catalogar con Oracle Recovery Manager (RMAN) para conservar la información de backups; estos backups se pueden utilizar posteriormente en operaciones de restauración a nivel de bloque o de recuperación a un momento específico de espacio de tabla.

Aspectos destacados de SnapManager

SnapManager integra perfectamente con las bases de datos Oracle en el host UNIX y es gracias a las tecnologías de copias Snapshot, SnapRestore y FlexClone de NetApp Ofrece una interfaz de usuario (UI) fácil de usar y una interfaz de línea de comandos (CLI) para funciones administrativas.

SnapManager permite realizar las siguientes operaciones de base de datos y gestionar los datos de forma eficiente:

- Creación de backups con gestión eficiente del espacio en almacenamiento primario o secundario

  SnapManager permite realizar backups de los archivos de datos y los archivos de registro de archivos por separado.

- Programación de backups
- Restauración de bases de datos completas o parciales mediante una operación de restauración basada en archivos o volúmenes
- Recuperación de bases de datos mediante la detección, el montaje y la aplicación de archivos de registro de archivos a partir de backups
- Eliminar archivos de registro de archivos de destinos de registro de archivos cuando se crean backups solo de los registros de archivos
- Si se conserva un número mínimo de backups de registros de archivos automáticamente, solo se deben retener los backups que contienen archivos únicos de registro de archivos
- Realizar un seguimiento de los detalles de las operaciones y generar informes
- Verificación de copias de seguridad para garantizar que las copias de seguridad tienen un formato de bloque válido y que ninguno de los archivos de copia de seguridad está dañado

- Mantener un historial de operaciones realizadas en el perfil de base de datos

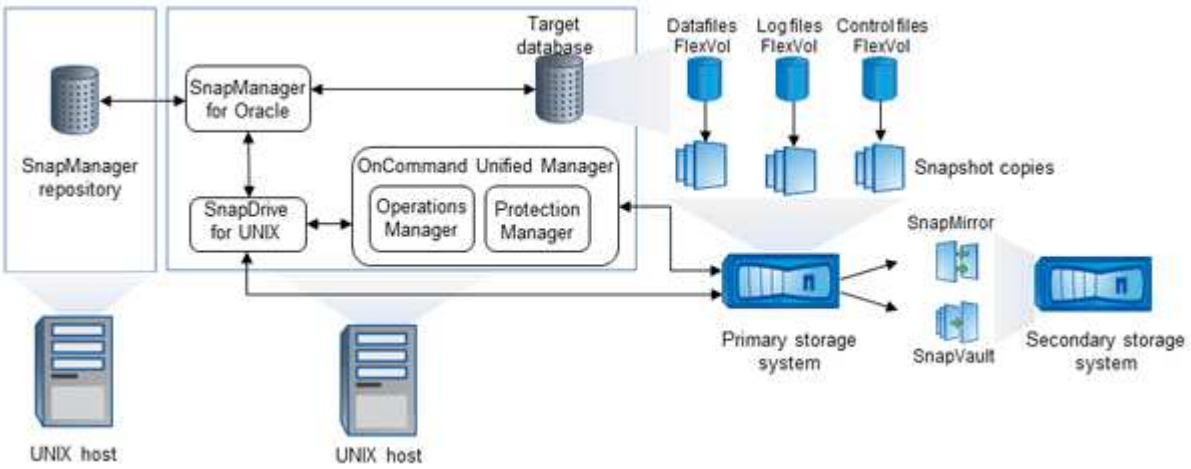
  Un perfil contiene información acerca de la base de datos que va a gestionar SnapManager.

- Protección de backups en sistemas de almacenamiento secundario y terciario.
- Crear clones de backups con gestión eficiente del espacio en el almacenamiento principal o secundario

  SnapManager permite dividir el clon de una base de datos.

Arquitectura SnapManager

SnapManager para Oracle incluye componentes que trabajan conjuntamente para proporcionar una solución completa y potente de backup, restauración, recuperación y clonación para bases de datos Oracle.



SnapDrive para UNIX

SnapManager requiere que SnapDrive establezca la conexión con el sistema de almacenamiento. Debe instalar SnapDrive para UNIX en cada host de la base de datos de destino antes de instalar SnapManager.

SnapManager para Oracle

Debe instalar SnapManager para Oracle en cada host de la base de datos de destino.

Es posible usar la interfaz de línea de comandos (CLI) o la interfaz de usuario desde el host de base de datos donde se ha instalado SnapManager para Oracle. También puede usar la interfaz de usuario de SnapManager de forma remota mediante un explorador web desde cualquier sistema que se ejecute en un sistema operativo compatible con SnapManager.

Las versiones de JRE compatibles son 1.5, 1.6, 1.7 y 1.8.

Base de datos de destino

La base de datos de destino es una base de datos de Oracle que se desea gestionar mediante SnapManager para realizar operaciones de backup, restauración, recuperación y clonado.

La base de datos de destino puede ser independiente, Real Application Clusters (RAC) o residir en volúmenes de Oracle Automatic Storage Management (ASM). Para obtener detalles sobre las versiones, las

configuraciones, los sistemas operativos y los protocolos de la base de datos de Oracle admitidos, consulte la herramienta de matriz de interoperabilidad de NetApp.

Repositorio de SnapManager

El repositorio de SnapManager reside en una base de datos de Oracle y almacena metadatos sobre perfiles, backups, restauración, recuperación y clonado. Un único repositorio puede contener información sobre las operaciones realizadas en varios perfiles de base de datos.

El repositorio de SnapManager no puede residir en la base de datos de destino. La base de datos del repositorio de SnapManager y la base de datos de destino deben estar en línea antes de ejecutar operaciones de SnapManager.

Paquete Core de OnCommand Unified Manager

El paquete principal de OnCommand Unified Manager integra las funcionalidades de Operations Manager, Protection Manager y Provisioning Manager. Centraliza las normativas de aprovisionamiento, clonado, backup y recuperación de datos, así como las de recuperación tras siniestros (DR). Integrar todas estas funciones hace que sea posible realizar muchas funciones de gestión desde una única herramienta.

Operations Manager

Operations Manager es la interfaz de usuario web del paquete principal de OnCommand Unified Manager. Se utiliza para la supervisión diaria del almacenamiento, las alertas de problemas y la generación de informes sobre la infraestructura del sistema de almacenamiento y el sistema de almacenamiento. La integración de SnapManager aprovecha las funcionalidades RBAC de Operations Manager.

Protection Manager

Protection Manager brinda a los administradores una consola de gestión fácil de usar que permite configurar y controlar rápidamente todas las operaciones de SnapMirror y SnapVault. La aplicación permite que los administradores apliquen políticas de protección de datos sistemáticas, automaticen procesos complejos de protección de datos y agrupen los recursos de respaldo y replicación para lograr una mejor utilización.

La interfaz de Protection Manager es la consola de gestión de NetApp, la plataforma de cliente para las aplicaciones de software de gestión de NetApp. La consola de gestión de NetApp se ejecuta en un sistema Windows o Linux diferente al servidor en el que se ha instalado el OnCommand Server. Permite a los administradores de almacenamiento, aplicaciones y servidores realizar tareas diarias sin tener que cambiar entre diferentes IU. Las aplicaciones que se ejecutan en la consola de gestión de NetApp son Protection Manager, Provisioning Manager y Performance Advisor.

Sistema de almacenamiento primario

SnapManager realiza un backup de las bases de datos objetivo en el sistema de almacenamiento primario de NetApp.

Sistema de almacenamiento secundario

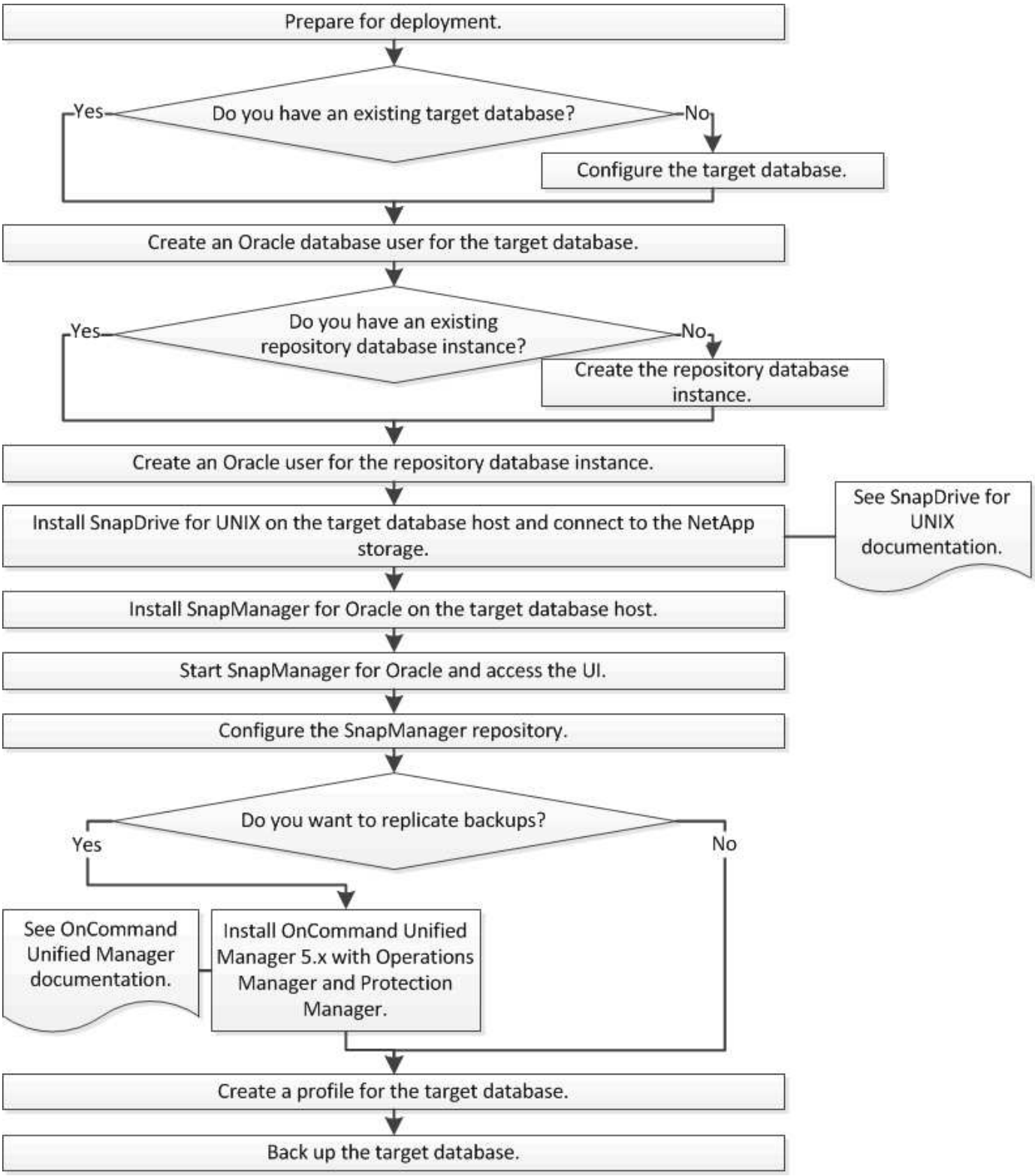
Cuando se habilita la protección de datos en un perfil de base de datos, los backups creados en el sistema de almacenamiento principal por SnapManager se replican en un sistema de almacenamiento secundario de NetApp mediante las tecnologías SnapVault y SnapMirror.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Flujo de trabajo de implementación

Antes de poder crear backups con SnapManager, primero debe instalar SnapDrive para UNIX y, a continuación, instalar SnapManager para Oracle.



Preparación para la implementación

Antes de implementar SnapManager, debe asegurarse de que el sistema de almacenamiento y los hosts UNIX cumplen con los requisitos mínimos de recursos.

1. Compruebe que tiene las licencias necesarias.
2. Compruebe las configuraciones admitidas.
3. Compruebe los tipos de almacenamiento admitidos.
4. Verificar que los hosts UNIX cumplen los requisitos de SnapManager.

Licencias de SnapManager

Se requieren una licencia de SnapManager y varias licencias de sistema de almacenamiento para habilitar las operaciones de SnapManager. La licencia de SnapManager está disponible en dos modelos de licencia: Por servidor, en el que la licencia de SnapManager reside en cada host de bases de datos y en las licencias por sistema de almacenamiento, en las que la licencia de SnapManager reside en el sistema de almacenamiento.

Los requisitos de licencia de SnapManager son los siguientes:

Licencia	Descripción	Donde se la requiere
SnapManager por servidor	Una licencia del lado del host para un host de base de datos específico. Las licencias solo son obligatorias para los hosts de base de datos en los que está instalado SnapManager. No se requiere ninguna licencia de SnapManager para el sistema de almacenamiento.	En el host SnapManager. No se requiere una licencia de SnapManager en los sistemas de almacenamiento primarios y secundarios al usar la licencia por servidor.
SnapManager por sistema de almacenamiento	Una licencia del almacenamiento compatible con cualquier número de hosts de base de datos. Es obligatorio solo si no utiliza una licencia por servidor en el host de la base de datos.	En sistemas de almacenamiento principales y secundarios
SnapRestore	Una licencia requerida que permite a SnapManager restaurar bases de datos.	En sistemas de almacenamiento principales y secundarios Requerida en sistemas de destino de SnapVault para restaurar un archivo a partir de un backup

Licencia	Descripción	Donde se la requiere
FlexClone	Una licencia opcional para clonar bases de datos.	En sistemas de almacenamiento principal y secundario.requerida en sistemas de destino de SnapVault al crear clones a partir de un backup.
SnapMirror	Una licencia opcional para reflejar backups en un sistema de almacenamiento de destino.	En sistemas de almacenamiento principales y secundarios
SnapVault	Una licencia opcional para archivar backups en un sistema de almacenamiento de destino.	En sistemas de almacenamiento principales y secundarios
Protocolos	Se requieren licencias de NFS, iSCSI o FC en función del protocolo utilizado.	En sistemas de almacenamiento principales y secundarios Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible

Configuraciones admitidas

Los hosts en los que está instalando SnapManager deben cumplir con los requisitos especificados de software, explorador, base de datos y sistema operativo. Debe verificar la compatibilidad de la configuración antes de instalar o actualizar SnapManager.

Para obtener información sobre las configuraciones admitidas, consulte la herramienta de matriz de interoperabilidad.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Tipos de almacenamiento admitidos

SnapManager admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Es necesario verificar la compatibilidad de su tipo de almacenamiento antes de instalar o actualizar SnapManager.

Máquina	Tipo de almacenamiento
Servidor físico	• Volúmenes conectados en NFS • LUN conectados a FC • LUN conectados a iSCSI

Máquina	Tipo de almacenamiento
ESX de VMware	• Volúmenes NFS conectados directamente con el Guest VM • LUN de RDM en el sistema operativo invitado

Requisitos del host UNIX

Debe instalar SnapManager para Oracle en cada host donde esté alojada una base de datos de Oracle que desee realizar el backup. Debe asegurarse de que los hosts cumplan con los requisitos mínimos de la configuración de SnapManager.

- Debe instalar SnapDrive en el host de la base de datos antes de instalar SnapManager.
- Puede instalar SnapManager en equipos físicos o virtuales.
- Debe instalar la misma versión de SnapManager en todos los hosts que compartan el mismo repositorio.
- Debe instalar Oracle Patch 13366202 si utiliza bases de datos Oracle 11.2.0.2 o 11.2.0.3.

  Si utiliza DNFS, también debe instalar los parches enumerados en el informe de My Oracle Support (MOS) 1495104.1 para obtener el máximo rendimiento y estabilidad.

Configurar bases de datos

Debe configurar al menos dos bases de datos de Oracle: Una base de datos de destino para la que se desea realizar un backup con SnapManager y una base de datos de repositorio para almacenar los metadatos de la base de datos de destino. La base de datos de destino y la base de datos del repositorio de SnapManager deben estar configuradas y en línea antes de ejecutar operaciones de SnapManager.

Configurar la base de datos de destino

La base de datos de destino es una base de datos de Oracle que se puede configurar como independiente, Real Application Clusters (RAC), Automatic Storage Management (ASM) o cualquier otra combinación compatible.

1. Configure la base de datos de destino haciendo referencia a *TR-3633*.

Información relacionada

"Informe técnico de NetApp 3633: Mejores prácticas para las bases de datos de Oracle en el almacenamiento de NetApp"

Crear un usuario de base de datos de Oracle para la base de datos de destino

Se necesita un usuario de la base de datos de Oracle para iniciar sesión en la base de datos y ejecutar operaciones de SnapManager. Debe crear este usuario con el privilegio *sysdba* si no existe un usuario con el privilegio *sysdba* para la base de datos de destino.

SnapManager puede utilizar cualquier usuario de Oracle con el privilegio *sysdba* que existe para la base de datos de destino. Por ejemplo, SnapManager puede utilizar el usuario predeterminado *sys*. Sin embargo, incluso si el usuario existe, puede crear un nuevo usuario para la base de datos de destino y asignar el privilegio *sysdba*.

También puede usar el método de autenticación del SO en donde el sistema operativo (SO) permite que la base de datos Oracle utilice las credenciales que mantiene el sistema operativo para autenticar a los usuarios para iniciar sesión en la base de datos y ejecutar operaciones de SnapManager. Si el sistema operativo autentica, puede conectarse a la base de datos de Oracle sin especificar un nombre de usuario o una contraseña.

1. Iniciar sesión en SQL *Plus: 'Sqlplus / as sysdba'
2. Cree un nuevo usuario con una contraseña de administrador: 'Cree useruser_name identificado por admin_password;'

   user_name es el nombre de usuario que va a crear y admin_password es la contraseña que desea asignar al usuario.

3. Asigne el privilegio sysdba al nuevo usuario de Oracle: 'GRANT sysdba to user_name;'

Crear la instancia de la base de datos del repositorio

La instancia de la base de datos del repositorio es una base de datos de Oracle en la que se crea el repositorio de SnapManager. La instancia de la base de datos del repositorio debe ser una base de datos independiente y no puede ser la base de datos de destino.

Debe tener una base de datos de Oracle y una cuenta de usuario para acceder a la base de datos.

1. Iniciar sesión en SQL *Plus: 'Sqlplus / as sysdba'
2. Cree un nuevo tablespace para el repositorio de SnapManager: 'Create tablespacetablenespace_name DataFile '/u01/app/oracle/oradata/DataFile/tablespace_name.dbf' size 100M autoextense activada;'

   tablespace_name es el nombre del tablespace.

3. Verifique el tamaño de bloque del tablespace: 'SELECT tablespace_name, block_size from dba_tablespaces;'

   SnapManager requiere un tamaño de bloque mínimo de 4 K para el espacio de tabla.

Información relacionada

"Informe técnico de NetApp 3761: "SnapManager para Oracle: Prácticas recomendadas"'

Crear un usuario de Oracle para la instancia de la base de datos del repositorio

Se necesita un usuario de Oracle para iniciar sesión en la instancia de la base de datos del repositorio y acceder a ella. Debe crear este usuario con privilegios *connect* y *resource*.

1. Iniciar sesión en SQL *Plus: 'Sqlplus / as sysdba'

2. Cree un nuevo usuario y asigne una contraseña de administrador a ese usuario: 'Create useruser_name identificado por admin_password Default tablespace_name quota ilimitada en tablespace_name;'
   - user_name es el nombre de usuario que va a crear para la base de datos del repositorio.
   - admin_password es la contraseña que desea asignar al usuario.
   - tablespace_name es el nombre del tablespace creado para la base de datos del repositorio.
3. Asigne los privilegios *connect* y *resource* al nuevo usuario de Oracle: 'Grant connect, resource to user_name;'

Verificación de la configuración del listener de Oracle

El listener es un proceso que escucha las solicitudes de conexión de cliente. Recibe solicitudes entrantes de conexión de cliente y administra el tráfico de estas solicitudes a la base de datos. Antes de conectarse a una base de datos de destino o a una instancia de base de datos de repositorio, puede utilizar el comando STATUS para comprobar la configuración del listener.

El comando STATUS muestra información básica sobre el estado de un listener específico, incluyendo un resumen de la configuración del listener, las direcciones del protocolo de escucha y un resumen de los servicios registrados con ese listener.

1. Introduzca el siguiente comando en el símbolo del sistema: 'Lsnrctl STATUS'

   El valor predeterminado asignado al puerto de escucha es 1521.

Instalando SnapManager

Debe instalar SnapManager en cada host donde se ejecute la base de datos de la que desea realizar el backup.

Debe haber instalado SnapDrive para UNIX en el host de la base de datos y establecer una conexión con el sistema de almacenamiento.

Para obtener información sobre cómo instalar SnapDrive y establecer una conexión con el sistema de almacenamiento, consulte la documentación de SnapDrive para UNIX.

Debe instalar una instancia de SnapManager por cada host de bases de datos. Si usa una base de datos de RAC y desea realizar un backup de la base de datos de RAC, debe instalar SnapManager en todos los hosts de la base de datos de RAC.

1. Descargue el paquete de instalación de SnapManager para Oracle para UNIX desde el sitio de soporte de NetApp y cópielo al sistema host.

   "Descargas de NetApp: "Software""

2. Inicie sesión en el host de la base de datos como usuario root.
3. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el paquete de instalación.
4. Haga ejecutable el paquete de instalación: Chmod 755install_package.bin
5. Install SnapManager: './install_package.bin'

6. Pulse Intro para continuar.
7. Siga estos pasos:
   a. Pulse Intro para aceptar el valor predeterminado para el grupo de sistemas operativos.

      El valor predeterminado para el grupo es dba.

   b. Pulse Intro para aceptar el valor predeterminado del tipo de inicio.

   Se muestra el resumen de la configuración.

8. Revise el resumen de la configuración y pulse Intro para continuar.

   SnapManager se instala en

Información relacionada

Configurar SnapManager

"Documentación de NetApp: "SnapDrive para UNIX"'

Configurar SnapManager

Puede iniciar SnapManager y acceder a ella mediante la interfaz de usuario (UI) o desde la interfaz de línea de comandos (CLI). Después de acceder a SnapManager, debe crear el repositorio de SnapManager antes de realizar cualquier operación de SnapManager.

Iniciando el servidor SnapManager

Debe iniciar el servidor SnapManager desde el host de la base de datos de destino.

1. Inicie sesión en el host de la base de datos de destino e inicie el servidor SnapManager:

   Aparece el siguiente mensaje: "Servidor SnapManager iniciado en puerto seguro Port_number con PID_Number".

   > El puerto predeterminado es 27214.

Puede verificar que SnapManager funciona correctamente:

Aparece el siguiente mensaje: 'Operation ID operation_ID_Number succeeded'.

Obtener acceso a la interfaz de usuario de SnapManager

Puede acceder a la interfaz de usuario de SnapManager de forma remota mediante un explorador web desde cualquier sistema que se ejecute en un sistema operativo compatible con SnapManager. También puede acceder a la interfaz de usuario de SnapManager desde el host de la base de datos de destino ejecutando el comando smogui.

- Debe asegurarse de que SnapManager esté en ejecución.
- Debe asegurarse de que el sistema operativo y Java compatibles estén instalados en el sistema donde desea acceder a la interfaz de usuario de SnapManager.

  Para obtener información sobre el sistema operativo compatible y Java, consulte herramienta matriz de interoperabilidad.

  a. En la ventana del navegador web, introduzca lo siguiente:https://server_name.domain.com:port_number[]
     - Server_name es el nombre del host de la base de datos de destino donde está instalado SnapManager.

       También puede introducir la dirección IP del host de la base de datos de destino.

     - Port_number es el puerto en el que se ejecuta SnapManager.

       El valor predeterminado es 27214.

  b. Haga clic en el vínculo.

     Se muestra la interfaz de usuario de.

Configurar el repositorio de SnapManager

Debe configurar el repositorio de SnapManager en la instancia de la base de datos del repositorio. La base de datos del repositorio almacena metadatos para las bases de datos gestionadas por SnapManager.

- Debe haber creado la instancia de la base de datos del repositorio.
- Debe haber creado el usuario de Oracle para la instancia de la base de datos del repositorio con los privilegios correspondientes.
- Debe haber incluido los detalles de la instancia de la base de datos del repositorio en el archivo tnsnames.ora.

Es posible configurar el repositorio de SnapManager desde la interfaz de usuario de SnapManager o desde la interfaz de línea de comandos (CLI). Estos pasos muestran cómo crear un repositorio con la interfaz de usuario de SnapManager. También puede utilizar la CLI si lo prefiere.

Para obtener información acerca de cómo crear el repositorio mediante la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el panel izquierdo de la interfaz de usuario de SnapManager, haga clic con el botón derecho del ratón en **repositorios**.
2. Seleccione **Crear nuevo repositorio** y haga clic en **Siguiente**.
3. En la ventana Repository Database Configuration Information (Información de configuración de la base de datos del repositorio), introduzca la siguiente información:

En este campo…	Realice lo siguiente…
Nombre de usuario	Introduzca el nombre del usuario creado para la instancia de la base de datos del repositorio.
Contraseña	Introduzca la contraseña.
Host	Introduzca la dirección IP del host donde se crea la instancia de la base de datos del repositorio.
Puerto	Introduzca el puerto utilizado para conectarse a la instancia de la base de datos del repositorio. El puerto predeterminado es 1521.
Nombre del servicio	Introduzca el nombre que utiliza SnapManager para conectarse a la instancia de la base de datos del repositorio. Dependiendo de los detalles incluidos en el archivo tnsnames.ora, puede ser el nombre corto del servicio o el nombre completo del servicio. +

4. En la ventana realizar operación de adición del repositorio, revise el resumen de configuración y haga clic en **Agregar**.

   Si la operación falla, haga clic en la pestaña **Detalles de operación** para ver qué causó el error de la operación. Los detalles del error también se capturan en el registro de operaciones ubicado en /var/log/smo.

5. Haga clic en **Finalizar**.

   El repositorio aparece en el panel izquierdo bajo el árbol **repositorios**. Si no ve el repositorio, haga clic con el botón derecho del ratón en **repositorios** y haga clic en **Actualizar**.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Realizar backup y verificación de las bases de datos

Después de instalar SnapManager, puede crear una copia de seguridad básica de la base de datos y comprobar que la copia de seguridad no contiene ningún archivo dañado.

Información relacionada

Información general sobre backup de SnapManager

Definición de una estrategia de backup

Crear un perfil para la base de datos

Realizar una copia de seguridad de la base de datos

Verificación de los backups de las bases de datos

Programación de copias de seguridad periódicas

Información general sobre backup de SnapManager

SnapManager utiliza la tecnología Snapshot de NetApp para crear backups de bases de datos. Puede utilizar la utilidad DBVERIFY o SnapManager para verificar la integridad de las copias de seguridad.

SnapManager realiza un backup de una base de datos mediante la creación de copias Snapshot de los volúmenes que contienen archivos de datos, archivos de control y archivos de registro de archivos. Juntas, estas copias Snapshot incluyen un conjunto de respaldos que SnapManager puede usar para restaurar una base de datos.

Definición de una estrategia de backup

Definir una estrategia de backup antes de crear backups garantiza que se cuente con todos los backups para restaurar correctamente las bases de datos. SnapManager ofrece un programa de backup granular y flexible para cumplir con el acuerdo de nivel de servicio.

Para obtener información sobre las prácticas recomendadas de SnapManager, consulte *TR 3761*.

¿Qué modo de backup de SnapManager necesita?

SnapManager admite dos modos de backup:

Modo de backup	Descripción
Backup en línea	Crea un backup de la base de datos cuando la base de datos está en estado en línea. Este modo de backup también se denomina backup dinámico.
Backup sin conexión	Crea un backup de la base de datos cuando la base de datos está en estado montado o apagado. Este modo de backup también se denomina backup en frío.

¿Qué tipo de backup de SnapManager necesita?

SnapManager admite tres tipos de backups:

Tipo de backup	Descripción
Backup completo	Crea un backup de la base de datos completa, que incluye todos los archivos de datos, los archivos de control y los archivos de registro de archivos.
Copia de seguridad parcial	Crea un backup de archivos de datos, archivos de control, espacios de tabla y archivos de registro de archivos seleccionados
Backup de solo registro de archivo	Crea una copia de seguridad sólo de los archivos de registro de archivo.debe seleccionar **copia de seguridad de archivos por separado** mientras crea el perfil.

¿Qué tipo de perfil de base de datos necesita?

SnapManager crea backups según si el perfil de la base de datos separa los backups de los registros de archivo de los backups del archivo de datos.

Tipo de perfil	Descripción
Un único perfil de base de datos para el backup combinado de archivos de datos y registros de archivos	Permite crear: • Backup completo que contiene todos los archivos de datos, los archivos de registro del archivo y los archivos de control • Backup parcial con los archivos de datos, espacios de tabla, archivos de registro de archivo y archivos de control seleccionados
Perfiles de base de datos separados para backups de registros de archivo y backups de archivos de datos	Permite crear: • Backup combinado con distintas etiquetas para backup de archivos de datos y backup de registros de archivo • Backup de solo archivos de datos de todos los archivos de datos junto con los archivos de control • Backup parcial de solo archivos de datos de los archivos de datos o espacios de tablas seleccionados junto con los archivos de control • Backup de solo registros de archivo

¿Qué convenciones de nomenclatura se deben utilizar para las copias Snapshot?

Las copias Snapshot creadas por los backups pueden seguir una convención de nomenclatura personalizada. El texto personalizado o las variables integradas, como el nombre del perfil, el nombre de la base de datos y el SID de la base de datos proporcionado por SnapManager, se pueden utilizar para crear la convención de nomenclatura. Puede crear la convención de nomenclatura mientras crea la política.

> Debe incluir la variable smid en el formato de nomenclatura. La variable smid crea un identificador de instantánea único.

La convención de nomenclatura de las copias Snapshot se puede cambiar durante o después de la creación de un perfil. El patrón actualizado se aplica solo a las copias Snapshot que todavía no se han creado; las copias Snapshot existentes conservan el patrón anterior.

¿Cuánto tiempo desea retener las copias de backup en el sistema de almacenamiento primario y en el sistema de almacenamiento secundario?

Una política de retención de backup especifica la cantidad de backups correctos que se retendrán. Puede especificar la política de retención mientras crea la política.

Puede seleccionar cada hora, día, semana, mensual o ilimitado como clase de retención. Para cada clase de retención, puede especificar el recuento de retención y la duración de la retención, ya sea de forma conjunta o individual.

- El recuento de retenciones determina la cantidad mínima de backups de una clase de retención determinada que se deben retener.

  Por ejemplo, si la programación de backup es *Daily* y el recuento de retenciones es *10*, se conservan 10 backups diarios.

  > El número máximo de copias de Snapshot que Data ONTAP permite retener es de 255. Cuando alcance el límite máximo, se producirá un error al crear nuevas copias Snapshot de forma predeterminada. Sin embargo, puede configurar la política de rotación en Data ONTAP para eliminar copias Snapshot más antiguas.

- La duración de la retención determina la cantidad mínima de días durante los cuales se debe conservar el backup.

  Por ejemplo, si la programación de la copia de seguridad es *Daily* y la duración de la retención es *10*, se retienen 10 días de los backups diarios.

Si se configura la replicación de SnapMirror, la política de retención se refleja en el volumen de destino.

> Para la retención a largo plazo de copias de backup, es conveniente usar SnapVault.

¿Desea verificar las copias de backup con el volumen de origen o un volumen de destino?

Si usa SnapMirror o SnapVault, puede verificar las copias de backups con la copia de Snapshot en el volumen de destino de SnapMirror o SnapVault, en lugar de la copia de Snapshot en el sistema de almacenamiento principal. Al utilizar un volumen de destino para verificar, se reduce la carga para el sistema de almacenamiento principal.

Información relacionada

"Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

Crear un perfil para la base de datos

Debe crear un perfil para que la base de datos pueda realizar cualquier operación en esa

base de datos. El perfil contiene información acerca de la base de datos y sólo puede hacer referencia a una base de datos; sin embargo, varios perfiles pueden hacer referencia a una base de datos. No es posible acceder a una copia de seguridad creada con un perfil desde otro perfil, incluso si ambos perfiles están asociados con la misma base de datos.

Asegúrese de que los detalles de la base de datos objetivo se incluyan en el archivo /etc/oratab.

Estos pasos muestran cómo crear un perfil para la base de datos con la interfaz de usuario de SnapManager. También puede utilizar la CLI si lo prefiere.

Para obtener información acerca de cómo crear perfiles mediante la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el árbol repositorios, haga clic con el botón secundario del ratón en el repositorio o en el host y seleccione **Crear perfil**.
2. En la página Información de configuración del perfil, introduzca el nombre y la contraseña personalizados del perfil.
3. En la página Database Configuration Information, introduzca la siguiente información:

En este campo…	Realice lo siguiente…
Nombre de la base de datos	Introduzca el nombre de la base de datos de la que desea realizar backup.
SID de base de datos	Introduzca el ID seguro (SID) de la base de datos. El nombre de la base de datos y el SID de la base de datos pueden ser iguales.
Host	Introduzca la dirección IP del host en el que reside la base de datos de destino. También puede especificar el nombre de host si el nombre de host se especifica en el sistema de nombres de dominio (DNS).
Cuenta de host	Introduzca el nombre de usuario de Oracle de la base de datos de destino. el valor predeterminado para el usuario es oracle.
Grupo de hosts	Introduzca el nombre del grupo de usuarios de Oracle. El valor predeterminado es dba. +

4. En la página Database Connection Information, seleccione una de las siguientes opciones:

Elija esto…	Si desea…
Usar autenticación de o/S	Utilice las credenciales que mantiene el sistema operativo para autenticar a los usuarios que acceden a la base de datos.
Usar autenticación de base de datos	Permitir que Oracle autentique un usuario administrativo mediante la autenticación del archivo de contraseña. Introduzca la información de conexión de la base de datos adecuada. • En el campo **SYSDBA Privileged User Name**, introduzca el nombre del administrador de la base de datos con privilegios administrativos. • En el campo **Contraseña**, introduzca la contraseña del administrador de la base de datos. • En el campo **Puerto**, introduzca el número de puerto utilizado para conectarse al host en el que reside la base de datos. El valor predeterminado es .
Usar autenticación de instancia de ASM	Permitir que la instancia de la base de datos de Automatic Storage Management (ASM) autentique un usuario administrativo. Introduzca la información de autenticación de la instancia de ASM correspondiente. • En el campo **SYSDBA/SYSASM Privileged User Name**, introduzca el nombre de usuario del administrador de la instancia de ASM con privilegios administrativos. • En el campo **Contraseña**, introduzca la contraseña del administrador.

Nota: sólo puede seleccionar el modo de autenticación ASM si tiene una instancia ASM en el host de la base de datos.

5. En la página Información de configuración de RMAN, seleccione una de las siguientes opciones:

Elija esto…	Si…
No utilice RMAN	No se utiliza RMAN para gestionar las operaciones de backup y restauración.
Usar RMAN a través del archivo de control	Se gestiona el repositorio de RMAN mediante archivos de control.

Elija esto…	Si…
Usar RMAN a través del Catálogo de recuperación	Se gestiona el repositorio de RMAN mediante la base de datos de catálogo de recuperación. Introduzca el nombre de usuario que tiene acceso a la base de datos del catálogo de recuperación, la contraseña y el nombre del servicio de red de Oracle de la base de datos que gestiona la conexión de sustrato de red transparente (TNS). +

6. En la página Snapshot Naming Information, seleccione las variables para especificar un formato de nomenclatura para la copia Snapshot.

   Debe incluir la variable smid en el formato de nomenclatura. La variable smid crea un identificador de instantánea único.

7. En la página Policy Settings, realice lo siguiente:
   a. Introduzca el recuento y la duración de la retención para cada clase de retención.
   b. En la lista desplegable **Directiva de protección**, seleccione la directiva de Protection Manager.
   c. Si desea realizar una copia de seguridad de los registros de archivos por separado, active la casilla de verificación **copia de seguridad de archivos por separado**, especifique la retención y seleccione la política de protección.

      Puede seleccionar una política que sea diferente de la asociada para los archivos de datos. Por ejemplo, si seleccionó una de la política de Protection Manager para archivos de datos, puede seleccionar una política diferente de Protection Manager para los registros de archivos.

8. En la página Configure Notification Settings, especifique los ajustes de notificación por correo electrónico.
9. En la página Información de configuración del historial, seleccione una de las opciones para mantener el historial de operaciones de SnapManager.
10. En la página Perform Profile Create Operation, compruebe la información y haga clic en **Crear**.
11. Haga clic en **Finalizar** para cerrar el asistente.

    Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Realizar una copia de seguridad de la base de datos

Después de crear un perfil, debe realizar un backup de la base de datos. Se pueden programar backups recurrentes después del backup y la verificación iniciales.

Estos pasos muestran cómo crear un backup de la base de datos con la interfaz de usuario de SnapManager. También puede usar la interfaz de línea de comandos (CLI) si lo prefiere.

Para obtener información acerca de cómo crear copias de seguridad mediante la CLI, consulte la

SnapManager for Oracle Administration Guide for UNIX.

1. En el árbol repositorios, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos de la que desea realizar la copia de seguridad y seleccione **copia de seguridad**.
2. En **Label**, introduzca un nombre personalizado para la copia de seguridad.

   No debe incluir espacios ni caracteres especiales en el nombre. Si no se especifica un nombre, SnapManager crea automáticamente una etiqueta de backup.

   En SnapManager 3.4, es posible modificar la etiqueta de backup creada automáticamente por SnapManager. Puede editar las variables de configuración override.default.backup.pattern y new.default.backup.pattern para crear su propio patrón de etiqueta de copia de seguridad predeterminado.

3. Seleccione **permitir inicio o cierre de la base de datos, si es necesario** para modificar el estado de la base de datos, si es necesario.

   Esta opción garantiza que si la base de datos no está en el estado requerido para crear un backup, SnapManager automáticamente llevará la base de datos al estado deseado a fin de completar la operación.

4. En la página Database, Tablespaces o Datafiles to Backup, realice lo siguiente:
   a. Seleccione **copia de seguridad de archivos de datos** para realizar una copia de seguridad de la base de datos completa, los archivos de datos seleccionados o los tablespaces seleccionados.
   b. Seleccione **copia de seguridad Archivelogs** para realizar una copia de seguridad de los archivos de registro de archivos por separado.
   c. Seleccione **Prune Archivelogs** si desea eliminar los archivos de registro de archivos del sistema de archivos activo del que ya se ha realizado una copia de seguridad.

      Si está habilitado el área de recuperación de flash (FRA) para los archivos de registro de archivos, SnapManager no puede depurar los archivos de registro de archivos.

   d. Seleccione **proteger la copia de seguridad** si desea activar la protección de copia de seguridad.

      Esta opción sólo está activada si se ha seleccionado la directiva de protección al crear el perfil.

   e. Seleccione **proteger ahora** si desea proteger la copia de seguridad inmediatamente en el almacenamiento secundario reemplazando el programa de protección de Protection Manager.
   f. En la lista desplegable **Tipo**, seleccione el tipo de copia de seguridad (sin conexión o en línea) que desea crear.

      Si selecciona Auto, SnapManager crea un backup según el estado actual de la base de datos.

   g. En la lista desplegable **clase de retención**, seleccione la clase de retención.
   h. Active la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** si desea asegurarse de que los archivos de copia de seguridad no están dañados.
5. En la página Task Enabling, especifique si desea realizar tareas antes y después de que se completen las operaciones de backup.
6. En la página realizar operaciones de copia de seguridad, compruebe la información y haga clic en **copia de seguridad**.
7. Haga clic en **Finalizar** para cerrar el asistente.

Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Verificación de los backups de las bases de datos

Puede verificar la copia de seguridad de la base de datos para asegurarse de que los archivos de los que se ha realizado una copia de seguridad no estén dañados.

Si no ha seleccionado la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** al crear una copia de seguridad, debe realizar estos pasos manualmente para verificar la copia de seguridad. Sin embargo, si seleccionó esta casilla de comprobación, SnapManager verifica automáticamente el backup.

1. En el árbol **repositorios**, seleccione el perfil.
2. Haga clic con el botón derecho del ratón en la copia de seguridad que desee verificar y seleccione **verificar**.
3. Haga clic en **Finalizar**.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

   En el árbol **repositorio**, haga clic con el botón secundario del ratón en la copia de seguridad y, a continuación, haga clic en **Propiedades** para ver los resultados de la operación de verificación.

Es posible usar archivos de backup para realizar operaciones de restauración. Para obtener información acerca de cómo realizar operaciones de restauración con la interfaz de usuario de SnapManager, consulte *Ayuda en línea*. Si desea utilizar la interfaz de línea de comandos (CLI) para realizar operaciones de restauración, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

Programación de copias de seguridad periódicas

Es posible programar operaciones de backup para que los backups se inicien automáticamente a intervalos regulares. SnapManager permite programar backups por hora, día, semana, mes o una sola vez.

Es posible asignar varias programaciones de backup para una sola base de datos. Sin embargo, cuando se programen varios backups para la misma base de datos, se debe asegurarse de que no se hayan programado al mismo tiempo.

Estos pasos muestran cómo crear una programación de backups para la base de datos con la interfaz de usuario de SnapManager. También puede usar la interfaz de línea de comandos (CLI) si lo prefiere. Para obtener información acerca de cómo programar copias de seguridad utilizando la CLI, consulte la *SnapManager for Oracle Administration Guide for UNIX*.

1. En el árbol repositorios, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos para la que desea crear una programación de copia de seguridad y seleccione **copia de seguridad programada**.
2. En **Label**, introduzca un nombre personalizado para la copia de seguridad.

No debe incluir espacios ni caracteres especiales en el nombre. Si no se especifica un nombre, SnapManager crea automáticamente una etiqueta de backup.

En SnapManager 3.4, es posible modificar la etiqueta de backup creada automáticamente por SnapManager. Puede editar las variables override.default.backup.pattern y new.default.backup.patternconfiguration para crear su propio patrón de etiqueta de copia de seguridad predeterminado.

3. Seleccione **permitir inicio o cierre de la base de datos, si es necesario** para modificar el estado de la base de datos, si es necesario.

   Esta opción garantiza que si la base de datos no está en el estado requerido para crear un backup, SnapManager automáticamente llevará la base de datos al estado deseado a fin de completar la operación.

4. En la página Database, Tablespaces o Datafiles to Backup, realice lo siguiente:
   a. Seleccione **copia de seguridad de archivos de datos** para realizar una copia de seguridad de la base de datos completa, los archivos de datos seleccionados o los tablespaces seleccionados.
   b. Seleccione **copia de seguridad Archivelogs** para realizar una copia de seguridad de los archivos de registro de archivos por separado.
   c. Seleccione **Prune Archivelogs** si desea eliminar los archivos de registro de archivos del sistema de archivos activo del que ya se ha realizado una copia de seguridad.

      Si está habilitado el área de recuperación de flash (FRA) para los archivos de registro de archivos, SnapManager no puede depurar los archivos de registro de archivos.

   d. Seleccione **proteger la copia de seguridad** si desea activar la protección de copia de seguridad.

      Esta opción sólo está activada si se ha seleccionado la directiva de protección al crear el perfil.

   e. Seleccione **proteger ahora** si desea proteger la copia de seguridad inmediatamente en el almacenamiento secundario reemplazando el programa de protección de Protection Manager.
   f. En la lista desplegable **Tipo**, seleccione el tipo de copia de seguridad (sin conexión o en línea) que desea crear.

      Si selecciona Auto, SnapManager crea un backup según el estado actual de la base de datos.

   g. En la lista desplegable **clase de retención**, seleccione la clase de retención.
   h. Active la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** si desea asegurarse de que los archivos de copia de seguridad no están dañados.
5. En el campo **Nombre de programa**, introduzca un nombre personalizado de la programación.

   No debe incluir espacios en el nombre.

6. En la página Configure Backup Schedule, realice lo siguiente:
   a. En la lista desplegable **Perform this operation**, seleccione la frecuencia de la programación de copia de seguridad.
   b. En el campo **Fecha de inicio**, especifique la fecha en la que desea iniciar el programa de copia de seguridad.
   c. En el campo **Hora de inicio**, especifique la hora a la que desea iniciar el programa de copia de seguridad.

d. Especifique el intervalo en el que se crearán los backups.

   Por ejemplo, si ha seleccionado la frecuencia por hora y especifica el intervalo como 2, los backups se programarán cada 2 horas.

7. En la página Task Enabling, especifique si desea realizar tareas antes y después de que se completen las operaciones de backup.
8. En la página realizar operación de programación de copia de seguridad, compruebe la información y haga clic en **Programación**.
9. Haga clic en **Finalizar** para cerrar el asistente.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4 para Oracle"

A continuación, ¿dónde ir

Después de instalar SnapManager y crear correctamente un backup, puede utilizar SnapManager para realizar operaciones de restauración, recuperación y clonado. Además, se recomienda buscar información sobre otras funciones de SnapManager, como la programación, la gestión de operaciones de SnapManager y el mantenimiento del historial de operaciones.

Es posible encontrar más información sobre estas funciones, así como información específica de la versión de SnapManager, en la siguiente documentación, toda la cual está disponible en "Soporte de NetApp".

- "Guía de administración para UNIX de SnapManager 3.4 para Oracle"

  Describe cómo configurar y administrar SnapManager para Oracle. Los temas incluyen cómo configurar, realizar backup, restaurar y clonar bases de datos, realizar una protección secundaria, Además, una explicación de los comandos de la CLI e instrucciones sobre cómo actualizar y desinstalar el producto.

- "Notas de la versión de SnapManager 3.4 para Oracle"

  Describe nuevas funciones, problemas solucionados, precauciones importantes, problemas conocidos y limitaciones de SnapManager para Oracle.

- *Ayuda en línea de SnapManager para Oracle*

  Describe los procedimientos paso a paso para realizar diferentes operaciones de SnapManager mediante la interfaz de usuario de SnapManager.

  > El *Ayuda en línea* se integra con la interfaz de usuario de SnapManager y no está disponible en el sitio de soporte.

- "Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

  Describe las prácticas recomendadas de SnapManager para Oracle.

- "Informe técnico de NetApp 3633: Mejores prácticas para las bases de datos de Oracle en el almacenamiento de NetApp"

  Describe las prácticas recomendadas para configurar las bases de datos de Oracle en el sistema de almacenamiento de NetApp.

Información relacionada

"Soporte de NetApp"

"Documentación de NetApp: Biblioteca de productos A-Z"

Guía de administración para UNIX®

En esta guía se describe cómo administrar SnapManager 3.4.2 para Oracle en un entorno UNIX después de completar la implementación, incluido cómo configurar, actualizar y desinstalar el producto, cómo realizar backup de bases de datos, restaurarlas y clonarlas.

Información general del producto

SnapManager para Oracle automatiza y simplifica los procesos manuales asociados a operaciones como el backup, la recuperación y el clonado de bases de datos de Oracle, tareas de gran complejidad y que requieren mucho tiempo. Puede usar SnapManager con la tecnología SnapMirror de ONTAP para crear copias de backups en otro volumen, y también con la tecnología ONTAP SnapVault para archivar backups de forma eficiente a disco.

SnapManager se integra con tecnologías nativas de Oracle como Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) y Direct NFS en protocolos FC, iSCSI y NFS. De manera opcional, los backups creados mediante SnapManager se pueden catalogar con Oracle RMAN para conservar la información de backups; estos backups se pueden utilizar posteriormente en operaciones de restauración a nivel de bloque o recuperación a un momento específico de espacio de tabla.

Aspectos destacados de SnapManager

SnapManager integra perfectamente con las bases de datos Oracle en el host UNIX y es gracias a las tecnologías de copias Snapshot, SnapRestore y FlexClone de NetApp Ofrece una interfaz de usuario (UI) fácil de usar y una interfaz de línea de comandos (CLI) para funciones administrativas.

SnapManager permite realizar las siguientes operaciones de base de datos y gestionar los datos de forma eficiente:

- Creación de backups con gestión eficiente del espacio en almacenamiento primario o secundario

  Es posible realizar un backup de los archivos de datos y los archivos de registro de archivos por separado.

- Programación de backups
- Restauración de bases de datos completas o parciales mediante una operación de restauración basada en archivos o volúmenes
- Recuperación de bases de datos mediante la detección, el montaje y la aplicación de archivos de registro de archivos a partir de backups
- Eliminar archivos de registro de archivos de destinos de registro de archivos cuando se crean backups solo de los registros de archivos
- Si se conserva un número mínimo de backups de registros de archivos automáticamente, solo se deben retener los backups que contienen archivos únicos de registro de archivos
- Realizar un seguimiento de los detalles de las operaciones y generar informes
- Verificación de copias de seguridad para garantizar que las copias de seguridad tienen un formato de bloque válido y que ninguno de los archivos de copia de seguridad está dañado

- Mantener un historial de operaciones realizadas en el perfil de base de datos

  Un perfil contiene información acerca de la base de datos que va a gestionar SnapManager.

- Crear clones de backups con gestión eficiente del espacio en sistemas de almacenamiento principales o secundarios

  SnapManager permite dividir el clon de una base de datos.

Crear backups usando copias de Snapshot

SnapManager permite crear backups en el almacenamiento primario (local) y en el almacenamiento secundario (remoto) mediante políticas de protección o scripts postprocesamiento.

Los backups que se crean como copias Snapshot son copias virtuales de la base de datos y se almacenan en el mismo medio físico que la base de datos. Por consiguiente, la operación de backup requiere menos tiempo y mucho menos espacio que los backups completos de disco a disco. SnapManager permite realizar el backup de los siguientes elementos:

- Todos los archivos de datos, los archivos de registro de archivo y los archivos de control
- Los archivos de datos o espacios de tablas seleccionados, todos los archivos de registro de archivo y los archivos de control

SnapManager 3.2 o posterior le permite realizar, opcionalmente, el backup de lo siguiente:

- Todos los archivos de datos y los archivos de control
- Los archivos de datos o tablespaces seleccionados junto con los archivos de control
- Archivos de registro de archivo

> Los archivos de datos, los archivos de registro de archivos y los archivos de control pueden ubicarse en diferentes sistemas de almacenamiento, volúmenes de sistema de almacenamiento y números de unidad lógica (LUN). También se puede usar SnapManager para realizar backup de una base de datos cuando hay varias bases de datos en el mismo volumen o LUN.

Por qué debe prune los archivos de registro de archivos

SnapManager para Oracle permite eliminar archivos de registro de archivos del sistema de archivos activo de del que ya se ha realizado un backup.

Eliminar permite a SnapManager crear backups de diferentes archivos de registro de archivos. Eliminar, junto con la política de retención de backups, libera espacio en los registros de archivos cuando se purgan los backups.

> No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos. Si especifica la ubicación del registro de archivos en el área de recuperación flash, debe asegurarse de especificar también la ubicación del registro de archivos en el parámetro archive_log_dest.

Consolidación de registros de archivo

SnapManager (3.2 o posterior) para Oracle consolida los backups de registros de archivos a fin de mantener una cantidad mínima de backups para los archivos de registro de archivos. SnapManager para Oracle identifica y libera los backups que contienen archivos de registros de archivos que son subconjuntos de otros backups.

Restauración total o parcial de bases de datos

SnapManager proporciona la flexibilidad necesaria para restaurar bases de datos completas, espacios de tablas específicos, archivos, archivos de control o una combinación de estas entidades. SnapManager le permite restaurar datos mediante un procesador de restauración basado en archivos un proceso de restauración más rápido y basado en volúmenes. Los administradores de bases de datos pueden seleccionar el proceso que desean utilizar o dejar que SnapManager decida qué proceso es apropiado.

SnapManager permite a los administradores de bases de datos obtener una vista previa de las operaciones de restauración. La función de vista previa permite a los administradores de bases de datos ver cada operación de restauración archivo por archivo.

Los administradores de bases de datos pueden especificar el nivel en el que SnapManager restaura y recupera la información cuando se ejecutan operaciones de restauración. Por ejemplo, los administradores de bases de datos pueden restaurar y recuperar datos en momentos específicos. El punto de restauración puede ser una fecha y hora, o un número de cambio de sistema (SCN) de Oracle.

Los administradores de bases de datos pueden usar SnapManager para restaurar la base de datos y usar otra herramienta para recuperar la información. Los administradores de bases de datos no tienen que usar SnapManager para ambas operaciones.

SnapManager (3.2 o posterior) permite restaurar y recuperar backups de bases de datos de forma automática sin intervención del administrador de base de datos. Es posible usar SnapManager para crear backups de registros de archivo, y luego usarlos para restaurar y recuperar los backups de bases de datos. Aunque los archivos de registro de archivo del backup se gestionen en una ubicación de un registro de archivo externo, puede especificar esa ubicación externa para que los registros de archivos puedan ayudar a recuperar la base de datos restaurada.

Comprobar el estado del backup

SnapManager puede confirmar la integridad del backup mediante las operaciones estándar de verificación de backup de Oracle.

Los administradores de bases de datos pueden realizar la verificación como parte de la operación de backup o al mismo tiempo. Los administradores de bases de datos pueden configurar la operación de verificación para que se produzca durante un tiempo de pico de actividad cuando la carga en los servidores host es menor o durante un período de mantenimiento programado.

Clones de backups de bases de datos

SnapManager utiliza la tecnología FlexClone para crear un clon modificable de un backup de base de datos con un uso eficiente del espacio. Es posible modificar un clon sin cambiar el origen de backup.

Quizás sería conveniente clonar bases de datos para permitir pruebas o actualizaciones en entornos no productivos. Es posible clonar una base de datos que reside en el almacenamiento secundario primor. Puede ubicarse un clon en el mismo host o en otro que la base de datos.

La tecnología FlexClone permite a SnapManager utilizar copias snapshot de la base de datos para evitar crear una copia física completa de disco a disco. Las copias Snapshot requieren menos tiempo de creación y ocupan mucho menos espacio que las copias físicas.

Consulte la documentación de Data ONTAP para obtener más información sobre la tecnología FlexClone.

Información relacionada

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

Realizar un seguimiento de los detalles y generar informes

SnapManager reduce el nivel de detalle que los administradores de las bases de datos necesitan para realizar un seguimiento del estado de las diferentes operaciones mediante la oferta de métodos para supervisar las operaciones desde una única interfaz.

Una vez que los administradores especifican qué bases de datos deben realizarse backups, SnapManager identifica automáticamente los archivos de la base de datos para el backup. SnapManager muestra información sobre repositorios, hosts, perfiles, backups y clones. Puede supervisar las operaciones en hosts o bases de datos específicos.también puede identificar los backups protegidos y determinar si los backups están en proceso o si están programados para producirse.

Qué repositorios son

SnapManager organiza la información en perfiles, que a continuación se asocian con repositorios. Los perfiles contienen información acerca de la base de datos que se está gestionando, mientras que el repositorio contiene datos acerca de las operaciones que se realizan en los perfiles.

El repositorio registra el momento en que se realizó un backup, qué archivos se hicieron de backup y si se creó un clon a partir del backup. Cuando los administradores de bases de datos restauran una base de datos o recuperan una parte del mismo, SnapManager consulta el repositorio para determinar qué se ha realizado un backup.

Como el repositorio almacena los nombres de las copias Snapshot de la base de datos creadas durante las operaciones de backup, la base de datos del repositorio no puede existir en la misma base de datos y tampoco puede formar parte de la misma base de datos de la que se realiza el backup de SnapManager. Debe tener al menos dos bases de datos (la base de datos del repositorio de SnapManager y la base de datos de destino que gestiona SnapManager) en funcionamiento cuando se ejecutan operaciones de SnapManager.

Si intenta abrir la interfaz gráfica de usuario (GUI) cuando la base de datos del repositorio está inactiva, se registra el siguiente mensaje de error en el archivo sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: No se han producido más datos para leer desde el socket. Además, se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva. Para obtener más información acerca de los diferentes mensajes de error, consulte *solución de problemas conocidos*.

Es posible usar cualquier nombre de host, nombre de servicio o nombre de usuario válido para realizar operaciones. Para que un repositorio admita operaciones SnapManager, el nombre de usuario y el nombre de servicio del repositorio sólo deben contener los siguientes caracteres: Caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-), guión bajo (_) y punto (.).

El puerto de repositorio puede ser cualquier número de puerto válido y el nombre de host del repositorio puede ser cualquier nombre de host válido. El nombre de host debe estar formado por caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-) y punto (.), pero no un guión bajo (_).

El repositorio debe crearse en una base de datos de Oracle. La base de datos que utiliza SnapManager debe configurarse de acuerdo con los procedimientos de Oracle para la configuración de la base de datos.

Un único repositorio puede contener información acerca de varios perfiles; sin embargo, cada base de datos normalmente se asocia a un único perfil. Puede tener varios repositorios, donde cada repositorio contiene varios perfiles.

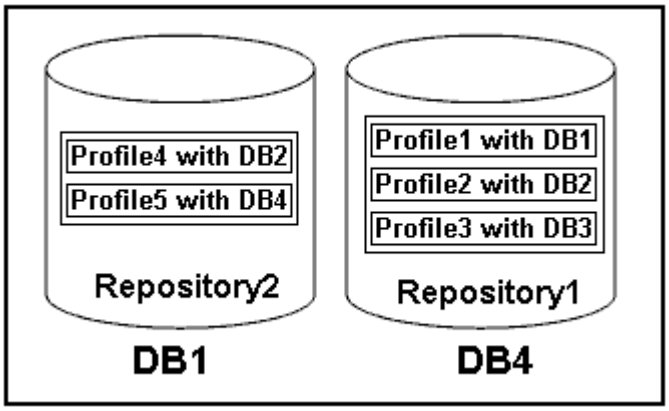
Qué perfiles son

SnapManager utiliza perfiles para almacenar la información necesaria para realizar operaciones en una base de datos determinada. Un perfil contiene información sobre la base de datos, incluidas sus credenciales, backups y clones. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos.

Un perfil sólo puede hacer referencia a una base de datos. Más de un perfil puede hacer referencia a la misma base de datos. No es posible acceder a los backups creados con un perfil desde otro perfil, aunque ambos perfiles hagan referencia a la misma base de datos.

La información del perfil se almacena en un repositorio. El repositorio contiene información de perfil de la base de datos e información sobre las copias de Snapshot que sirven como backup de base de datos. Las copias Snapshot reales se almacenan en el sistema de almacenamiento. Los nombres de las copias Snapshot se almacenan en el repositorio que contiene el perfil de esa base de datos. Cuando se realiza una operación en una base de datos, debe seleccionar el perfil en el repositorio.

La siguiente figura muestra cómo los repositorios pueden contener varios perfiles, pero también que cada perfil puede definir sólo una base de datos:



En el ejemplo anterior, deleteRepository2 se encuentra en la base de datos DB1 y deleteRepository1 en la base de datos DB4.

Cada perfil contiene las credenciales de la base de datos asociada al perfil. Las credenciales permiten que

SnapManager se conecte a la base de datos y trabaje con ella. Las credenciales almacenadas incluyen el nombre de usuario y las parejas de contraseñas para acceder al host, al repositorio, a la base de datos y a la información de conexión necesaria si utiliza Oracle Recovery Manager (RMAN).

No se puede acceder a un backup que se creó con un perfil de otro perfil, incluso si los dos perfiles están asociados con la misma base de datos. SnapManager coloca un bloqueo en la base de datos para evitar que se realicen dos operaciones incompatibles a la vez.

Perfil para crear copias de seguridad completas y parciales

Puede crear perfiles para realizar copias de seguridad completas o parciales.

Los perfiles que se especifican para crear las copias de seguridad completas y parciales contienen tanto los archivos de datos como los archivos de registro de archivos. SnapManager no permite que dichos perfiles separen los backups de registros de archivo de los backups del archivo de datos. Los backups completos y parciales se retienen en función de las políticas de retención de backup existentes y se protegen de acuerdo con las políticas de protección existentes. Puede programar copias de seguridad completas y parciales en función del tiempo y la frecuencia que mejor le convenga.

Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad de sólo registro de archivos

SnapManager (3.2 o posterior) permite crear perfiles para realizar backups de los archivos de registro de archivos independientemente de los archivos de datos. Después de usar el perfil para separar los tipos de backup, es posible crear backups de solo los archivos de datos o backups de solo registros de archivos de la base de datos. También es posible crear un backup que contenga los archivos de datos y los archivos de registro de archivos juntos.

La política de retención se aplica a todos los backups de la base de datos cuando no están separados los backups de registros de archivos. Después de separar los backups de registros de archivos, SnapManager permite especificar diferentes duraciones de retención y políticas de protección para los backups de registros de archivos.

Política de retención

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Una copia de seguridad caduca cuando su antigüedad supera el período de retención establecido para su clase de retención y la cantidad de backups supera el número de retención. Por ejemplo, si el número de backup es 15 (lo que significa que SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups más antiguos, correctos y elegibles caducan.

Duración de la retención del registro de archivo

Una vez separados los backups de los registros de archivos, se retienen en función de la duración de la retención de los registros de archivos. Los backups de registros de archivo que se realizan con los backups de archivos de datos siempre se conservan junto con estos backups de archivos de datos, independientemente de la duración de la retención de registros de archivo.

Información relacionada

Gestionar perfiles para backups eficientes

Qué son los estados de operación de SnapManager

Las operaciones de SnapManager (backup, restauración y clonado) pueden estar en diferentes estados y cada estado indica el progreso de la operación.

Estado de la operación	Descripción
Correcto	La operación se ha completado correctamente.
Ejecutando	La operación se inició, pero no ha finalizado. Por ejemplo, se programa que un backup, que tarda dos minutos, se lleve a cabo a las 11:00. Al ver la ficha **Programación** a las 11:01 a.m., la operación aparece como en ejecución.
No se ha encontrado ninguna operación	La programación no se ha ejecutado o se ha eliminado la última copia de seguridad ejecutada.
Error	Error en la operación. SnapManager ha ejecutado automáticamente el proceso de anulación y ha limpiado la operación. **Nota:** puede dividir el clon que se crea. Cuando se detiene la operación de división de clones que se inició y la operación se detiene correctamente, el estado de la operación de división de clones muestra como error.

Eventos recuperables e irrecuperables

Un evento SnapManager recuperable tiene los siguientes problemas:

- La base de datos no se almacena en un sistema de almacenamiento que ejecuta Data ONTAP.
- Se configuró una base de datos de Automatic Storage Management (ASM), pero no se está ejecutando la instancia de ASM.
- SnapDrive para UNIX no está instalado o no puede acceder al sistema de almacenamiento.
- SnapManager no puede crear una copia Snapshot o aprovisionar almacenamiento si el volumen no tiene espacio, se alcanzó el número máximo de copias Snapshot o se produce una excepción no prevista.

Cuando se produce un evento recuperable, SnapManager realiza un proceso de anulación e intenta devolver el host, la base de datos y el sistema de almacenamiento al estado inicial. Si el proceso de anulación falla, SnapManager trata el incidente como un evento irrecuperable.

Un evento irrecuperable (fuera de banda) se produce cuando se produce cualquiera de los siguientes acontecimientos:

- Se produce un problema con el sistema, como cuando se produce un error en un host.
- Se ha detenido el proceso SnapManager.
- Se produce un error en una operación de anulación en banda cuando el sistema de almacenamiento falla, el número de unidad lógica (LUN) o el volumen de almacenamiento están sin conexión o la red falla.

Cuando se produce un evento irrecuperable, SnapManager realiza un proceso de cancelación

inmediatamente. Es posible que el host, la base de datos y el sistema de almacenamiento no regresen a los estados iniciales. Si este es el caso, debe realizar una limpieza después de que la operación SnapManager falle; para ello, elimine la copia snapshot huérfana y elimine el archivo de bloqueo de SnapManager.

Si desea eliminar el archivo de bloqueo SnapManager, desplácese a $ORACLE_HOME en el equipo de destino y elimine el archivo sm_lock_TargetDBName. Después de eliminar el archivo, debe reiniciar SnapManager para Oracle Server.

Cómo mantiene SnapManager la seguridad

Es posible realizar operaciones de SnapManager solo si cuenta con las credenciales adecuadas. La seguridad en SnapManager está regida por la autenticación de usuarios y el control de acceso basado en roles (RBAC). RBAC permite que los administradores de bases de datos restrinjan las operaciones que SnapManager puede realizar en los volúmenes y LUN que contienen los archivos de datos de una base de datos.

Los administradores de bases de datos habilitan el RBAC para SnapManager mediante SnapDrive. A continuación, los administradores de bases de datos asignan permisos a los roles de SnapManager y asignan estos roles a los usuarios en la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) de Operations Manager. Las comprobaciones de permisos de RBAC se realizan en DataFabric Manager Server.

Además del acceso basado en roles, SnapManager mantiene la seguridad mediante la solicitud de autenticación de usuario mediante solicitudes de contraseña o la configuración de credenciales de usuario. Un usuario efectivo se autentica y autoriza con el servidor SnapManager.

Las credenciales de SnapManager y la autenticación de usuario difieren significativamente de SnapManager 3.0:

- En las versiones de SnapManager anteriores a la 3.0, debe establecer una contraseña de servidor arbitraria al instalar SnapManager. Cualquier persona que desee utilizar el servidor SnapManager necesitará la contraseña del servidor SnapManager. La contraseña del servidor SnapManager debería añadirse a las credenciales de usuario mediante el comando smo credential set -host.
- En SnapManager (3.0 y posterior), la contraseña del servidor SnapManager ha sido sustituida por la autenticación individual del sistema operativo (SO) de usuario. Si no ejecuta el cliente desde el mismo servidor que el host, el servidor SnapManager realiza la autenticación con los nombres de usuario y contraseñas del sistema operativo. Si no desea que se le soliciten las contraseñas de sistema operativo, puede guardar los datos en la caché de credenciales de usuario de SnapManager mediante el comando smo credential set -host.

> El comando smo credential set -host recuerda las credenciales cuando la propiedad host.credentials.persists del archivo smo.config está establecida en TRUE.

ejemplo

User1 y User2 comparten un perfil denominado Pro2. User2 no puede realizar una copia de seguridad de Database1 en Host1 sin permiso para acceder a Host1. User1 no puede clonar una base de datos a Host3 sin permiso para acceder a Host3.

En la siguiente tabla se describen los diferentes permisos asignados a los usuarios:

Tipo de permiso	Usuario1	Usuario2

Contraseña del host	Host1, Host2	Host2, Host3
Contraseña de repositorio	Repo. 1	Repo. 1
Contraseña de perfil	Pro1, Pro2	Profeca2

En caso de que User1 y User2 no tengan ningún perfil compartido, supongamos que User1 tiene permisos para los hosts denominados Host1 y Host2 y que User2 tiene permisos para el host denominado Host2. User2 no puede ejecutar ni siquiera los comandos que no son de perfil, como dump y verificación del sistema en Host1.

Acceso e impresión de la Ayuda en línea

La Ayuda en línea proporciona instrucciones para las tareas que puede realizar mediante la interfaz gráfica de usuario de SnapManager. La Ayuda en línea también proporciona descripciones de los campos de las ventanas y asistentes.

1. Ejecute una de las siguientes acciones:
   - En la ventana principal, haga clic en **Ayuda** > **Contenido de la Ayuda**.
   - En cualquier ventana o asistente, haga clic en **Ayuda** para ver la ayuda específica de esa ventana.
2. Utilice **Tabla de contenido** en el panel izquierdo para navegar por los temas.
3. Haga clic en el icono impresora situado en la parte superior de la ventana de ayuda para imprimir temas individuales.

Diseños generales de bases de datos y configuraciones de almacenamiento recomendados

Conocer los diseños generales recomendados de las bases de datos y las configuraciones de almacenamiento puede ayudarle a evitar problemas relacionados con los grupos de discos, los tipos de archivos y los espacios de tablas.

- No incluya archivos de más de un tipo de sistema de archivos SAN o administrador de volúmenes en la base de datos.

  Todos los archivos que conforman una base de datos deben residir en el mismo tipo de sistema de archivos.

- SnapManager requiere un gran tamaño de bloque de 4 KB.
- Incluyen el identificador del sistema de la base de datos en el archivo oratab.

  Incluir una entrada en el archivo oratab de cada base de datos que se gestionará. SnapManager utiliza el archivo oratab para determinar qué directorio raíz de Oracle usar.

- Para registrar backups de SnapManager en Oracle RMAN, debe crear perfiles habilitados para RMAN.

Si desea aprovechar la nueva restauración basada en volúmenes o la restauración de grupos de discos completos, tenga en cuenta las siguientes directrices relacionadas con los sistemas de archivos y los grupos de discos:

- Varias bases de datos no pueden compartir el mismo grupo de discos de Automatic Storage Management (ASM).
- Un grupo de discos que contiene archivos de datos no puede contener otros tipos de archivos.
- El número de unidad lógica (LUN) para el grupo de discos de archivos de datos debe ser el único objeto del volumen de almacenamiento.

A continuación se muestran algunas directrices para la separación de volúmenes:

- Los archivos de datos de una sola base de datos deben estar en el volumen.
- Debe utilizar volúmenes independientes para cada una de las siguientes clasificaciones de archivos: Archivos binarios de base de datos, archivos de datos, archivos redo log en línea, archivos redo log archivados y archivos de control.
- No es necesario crear un volumen separado para los archivos de base de datos temporales, ya que SnapManager no realiza backups de archivos de base de datos temporales.

Definir el inicio de la base de datos con el archivo oratab

SnapManager utiliza el archivo oratab durante las operaciones para determinar el directorio inicial de la base de datos de Oracle. Una entrada de la base de datos de Oracle debe estar en el archivo oratab para que SnapManager funcione correctamente. El archivo oratab se crea durante la instalación del software de Oracle.

El archivo oratab reside en diferentes ubicaciones según el sistema operativo del host, como se muestra en la siguiente tabla:

Sistema operativo del host	Ubicación del archivo
Linux	/etc/oratab
Solaris	/var/opt/oracle/oratab
IBM AIX	/etc/oratab

El archivo oratab de muestra contiene la siguiente información:

```
+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
```

Después de instalar Oracle, debe asegurarse de que el archivo oratab resida en la ubicación especificada en la tabla anterior. Si el archivo oratab no reside en la ubicación correcta por cada sistema operativo, debe comunicarse con el soporte técnico para obtener ayuda.

Requisitos para usar bases de datos de RAC con SnapManager

Debe conocer las recomendaciones para usar bases de datos de Real Application

Clusters (RAC) con SnapManager. Las recomendaciones incluyen números de puerto, contraseñas y modo de autenticación.

- En el modo de autenticación de la base de datos, el listener de cada nodo que interactúa con una instancia de la base de datos RAC debe configurarse para que utilice el mismo número de puerto.

  El listener que interactúa con la instancia de base de datos primaria debe iniciarse antes de iniciar el backup.

- En modo de autenticación del sistema operativo o en un entorno de ASM, se debe instalar y ejecutar el servidor SnapManager en cada nodo del entorno RAC.
- La contraseña de usuario de la base de datos (por ejemplo, para un administrador del sistema o un usuario con el privilegio sysdba) debe ser la misma para todas las instancias de la base de datos Oracle en un entorno RAC.

Requisitos para usar bases de datos de ASM con SnapManager

Debe conocer los requisitos para usar las bases de datos de gestión automática de almacenamiento (ASM) con SnapManager. Conocer estos requisitos puede ayudarle a evitar problemas con ASMLib, particiones y especificaciones de clonación, entre otras cosas.

- SnapManager (3.0.3 o posterior) utiliza el nuevo privilegio sysasm disponible con Oracle 11gR2 en lugar del privilegio sysdba para administrar una instancia de Oracle ASM.

  Si utiliza el privilegio sysdba para ejecutar comandos administrativos en la instancia de ASM, se muestra un mensaje de error. La base de datos utiliza el privilegio sysdba para acceder a los grupos de discos. Si se conecta a la instancia de ASM mediante el privilegio sysasm, tendrá acceso completo a todos los grupos de discos y funciones de administración de Oracle ASM disponibles.

  > Si utiliza Oracle 10gR2 y 11gR1, debe continuar utilizando el privilegio sysdba.

- SnapManager (3.0.3 o posterior) admite la copia de seguridad de bases de datos que se almacenan directamente en grupos de discos ASM cuando el grupo de discos también contiene un volumen de sistema automático de archivos de clúster (ACFS).

  Estos archivos están protegidos indirectamente por SnapManager y pueden restaurarse con el contenido restante de un grupo de discos de ASM, pero SnapManager (3.0.3 o posterior) no admite ACFS.

  > ACFS es una tecnología de gestión del almacenamiento del sistema de archivos escalable y multiplataforma disponible con Oracle 11gR2. ACFS amplía la funcionalidad ASM para admitir archivos de clientes que se mantienen fuera de la base de datos Oracle.

- SnapManager (3.0.3 o posterior) admite la copia de seguridad de archivos almacenados en grupos de discos ASM cuando el grupo de discos también contiene archivos de registro de cluster Oracle (OCR) o archivos de disco de votación; sin embargo, las operaciones de restauración requieren un método más lento, basado en host o de restauración instantánea de archivo parcial (PFSR).

  Es mejor tener discos OCR y de votación en grupos de discos que no contengan archivos de base de datos.

- Cada disco utilizado para ASM debe contener sólo una partición.

- La partición que aloja los datos de ASM debe estar correctamente alineada para evitar problemas graves de rendimiento.

  Esto implica que la LUN debe ser del tipo correcto y la partición debe tener un desplazamiento que es un múltiplo de 4K bytes.

  > Para obtener más información sobre cómo crear particiones alineadas con 4K, consulte el artículo 1010717 de Knowledge base.

- No se especifica la configuración de ASM como parte de la especificación del clon.

  Debe quitar manualmente la información de configuración de ASM en las especificaciones de clonado que se crearon con SnapManager 2.1 antes de actualizar el host a SnapManager (2.2 o posterior).

- SnapManager 3.1, 3.1p1 y 3.2 o posterior admiten ASMLib 2.1.4.
- SnapManager 3.1p4 o posterior admiten ASMLib 2.1.4, 2.1.7 y 2.1.8.

Dispositivos de partición compatibles

Debe conocer los diferentes dispositivos de partición compatibles con SnapManager.

La siguiente tabla proporciona información de partición y cómo se puede activar para diferentes sistemas operativos:

De NetApp	Partición única	Partición múltiple	Dispositivos sin partición	Sistema de archivos o dispositivos RAW
Red Hat Enterprise Linux 5x o 5 veces Oracle Enterprise Linux	Sí	No	No	ext3*
Red Hat Enterprise Linux 6xor 6 veces Oracle Enterprise Linux	Sí	No	No	ext3 o ext4*
SUSE Linux Enterprise Server 11	Sí	No	No	ext3*
SUSE Linux Enterprise Server 10	No	No	Sí	ext3***

De NetApp	Partición única	Partición múltiple	Dispositivos sin partición	Sistema de archivos o dispositivos RAW
Red Hat Enterprise Linux 5x o posterioresor Oracle Enterprise Linux 5 o posterior	Sí	No	Sí	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4or SUSE Linux Enterprise Server 11	Sí	No	Sí	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4 o posteror SUSE Linux Enterprise Server 11	Sí	No	No	ASM sin ASMLib**

Para obtener más información sobre las versiones compatibles del sistema operativo, consulte la matriz de interoperabilidad.

Compatibilidad con ASMLib

SnapManager admite diferentes versiones de ASMLib, aunque hay varios factores que debe tener en cuenta al utilizar SnapManager con ASMLib.

SnapManager admite ASMLib 2.1.4, 2.1.7 y 2.1.8. Todas las operaciones de SnapManager se pueden realizar con ASMLib 2.1.4, 2.1.7 y 2.1.8.

Si actualizó desde ASMLib 2.1.4 a ASM 2.1.7, es posible usar los mismos perfiles y backups creados con ASMLib 2.1.4 para restaurar los backups y crear los clones.

Debe tener en cuenta lo siguiente al utilizar SnapManager con ASMLib:

- SnapManager 3.1 no admite ASMLib 2.1.7.

  SnapManager 3.1p4 o posterior admiten ASMLib 2.1.4, 2.1.7 y 2.1.8.

- Después de realizar una actualización sucesiva desde SnapManager 3.1 a 3.2, las copias de seguridad creadas mediante ASMLib 2.1.7 funcionan únicamente si el repositorio se revierte a SnapManager 3.1 y ASMLib 2.1.7 se degrada a ASMLib 2.1.4.
- Después de realizar una actualización sucesiva desde SnapManager 3.1 a 3.2, las copias de seguridad creadas con ASMLib 2.1.7 no funcionan si el repositorio se revierte a SnapManager 3.1 con ASMLib 2.1.7.

  La reversión se realiza correctamente, pero no se pueden utilizar los perfiles y las copias de seguridad.

Compatibilidad con bases de datos de ASM sin ASMLib

SnapManager admite ASM sin ASMLib, de forma predeterminada. El requisito básico es que se deban particionar los dispositivos que se usan para los grupos de discos ASM.

Cuando ASMLib no está instalado, los permisos de dispositivo relacionados con los grupos de discos de ASM cambian a root:disk cuando se realizan las siguientes operaciones:

- Reinicie el host
- Restaure una base de datos desde el almacenamiento principal mediante SnapRestore (VBSR) basada en volúmenes.
- Restaurar una base de datos desde el almacenamiento secundario

Puede establecer los permisos de dispositivo adecuados asignando true a la variable de configuración oracleasm.support.without.asmlib en smo.conf. Los dispositivos relacionados con los grupos de discos ASM se agregan o eliminan del archivo initasmdisks cada vez que se agregan o eliminan nuevos dispositivos del host. El archivo initasmdisks está ubicado en /etc/initasmdisks.

Por ejemplo, si establece oracleasm.support.without.asmlib=true y, a continuación, realiza un montaje de copia de seguridad, se agregan nuevos dispositivos a initasmdisks. Cuando se reinicia el host, los scripts de inicio mantienen los permisos y la propiedad del dispositivo.

El valor predeterminado para oracleasm.support.without.asmlib es FALSE.

Información relacionada

Dispositivos de partición compatibles

Scripts compatibles

Los scripts asmmain.sh y asmquerydisk.sh permiten cambiar el usuario, el grupo y el usuario de la cuadrícula, todos los cuales se utilizan para consultar los discos ASM. Los scripts siempre deben ejecutarse desde la raíz.

El archivo asmmain.sh es el archivo de secuencia de comandos principal llamado desde cualquier operación que agregue o elimine dispositivos. La secuencia de comandos asmmain.sh llama internamente a otra secuencia de comandos, que debe ejecutarse desde la raíz que tiene las credenciales de la cuadrícula de oracle. Esta secuencia de comandos consulta los dispositivos del grupo de discos ASM y, a continuación, agrega esas entradas en el archivo initasmdisk con el permiso y la propiedad de los dispositivos. Puede cambiar los permisos y la propiedad de este archivo en función del entorno y del patrón regex que se utiliza para hacer coincidir sólo con /dev/mapper/*p1.

La secuencia de comandos asmquerydisk.sh se utiliza para consultar la lista de discos, que se utiliza para crear el grupo de discos ASM. Debe asignar valores a ORACLE_BASE, ORACLE_HOME y ORACLE_SID, según la configuración.

Los scripts están ubicados en /opt/NetApp/smo/plugins/examples/noasmlib. Sin embargo, estos scripts deben moverse a /opt/NetApp/smo/plugins/noasmlib antes de iniciar el servidor SnapManager para Oracle en el host.

Limitaciones de uso de scripts para admitir una base de datos ASM sin ASMLib

Debe tener en cuenta ciertas limitaciones al uso de scripts para admitir una base de

datos ASM sin ASMLib.

- Las secuencias de comandos ofrecen una solución alternativa para cualquier versión del kernel, pero sólo si ASMLib no está instalado.
- Los permisos de los scripts deben definirse de forma que los usuarios root, Grid, oracle o equivalentes puedan acceder a los scripts.
- Los scripts no admiten la restauración desde una ubicación secundaria.

Implementar y ejecutar los scripts

Es posible implementar y ejecutar los scripts asmmain.sh y asmquerydisk.sh para admitir bases de datos ASM sin ASMLib.

Estas secuencias de comandos no siguen la sintaxis de los scripts previos o posteriores y se llama al flujo de trabajo cuando los intitasmdiscos están habilitados. Puede cambiar cualquier cosa relacionada con la configuración en los scripts. Se recomienda verificar si todo lo contenido en los scripts funciona según lo esperado realizando una ejecución de secado rápida.

> Estas secuencias de comandos no afectan a su sistema en caso de fallos ni afectarán a su sistema. Estas secuencias de comandos se ejecutan para actualizar los discos relacionados con ASM para que tengan los permisos y la propiedad adecuados, de modo que los discos siempre estarán bajo control de instancia de ASM.

1. Cree los grupos de discos ASM con los discos con particiones.
2. Cree la base de datos Oracle en LOS GRUPOS de DISCOS.
3. Detenga el servidor SnapManager para Oracle.

   > En un entorno RAC, debe realizar este paso en todos los nodos de RAC.

4. Modifique smo.conf para incluir los siguientes parámetros:

   a. oracleasm.support.without.asmlib = true
   b. oracleasm.support.without.asmlib.owpropiedad = true
   c. oracleasm.support.without.asmlib.username = nombre de usuario del entorno de instancia de ASM
   d. oracleasm.support.without.asmlib.groupname = nombre de grupo del entorno de instancia de ASM

   Estas modificaciones establecen los permisos sólo para la ruta absoluta, lo que significa que en lugar del dispositivo de partición, los permisos se establecerán sólo para el dispositivo dm-*.

5. Modifique los scripts de los plugins disponibles en /opt/NetApp/smo/plugins/examples/noasmlib para incluir los ajustes de configuración en los scripts.
6. Copie las secuencias de comandos en /opt/NetApp/smo/plugins/noasmlib antes de iniciar el servidor SnapManager para Oracle en el host.
7. Desplácese hasta el directorio /opt/NetApp/smo y ejecute una ejecución en seco ejecutando el siguiente script: sh plugins/noasmlib/asmmain.sh

   Se crea el archivo etc/initasmdisks, que es el archivo principal que se utiliza.

   Puede confirmar que el archivo etc/initasmdisks contiene todos los dispositivos relacionados con la base de datos ASM configurada, como:

```
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. Inicie el servidor de SnapManager para Oracle.
9. Configure SnapDrive para UNIX añadiendo lo siguiente al archivo snapdrive.conf.disconnect-luns-before-vbsr=on
10. Reinicie el servidor de SnapDrive para UNIX.

En un entorno RAC, es necesario realizar los pasos del 3 al 10 para todos los nodos RAC.

El archivo /etc/initasmdisks creado, debe ejecutarse desde uno de los scripts de inicio o desde un script que se acaba de definir en rc3.d. El archivo /etc/initasmdisks debe ejecutarse siempre antes de que se inicie el servicio oracleha.

Ejemplo

```
# 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
```

En el ejemplo siguiente, sh -x/etc/initasmdisks no estará disponible de forma predeterminada, y debe anexarlo como primera línea de la función `start_stack()` en un script ohasd:

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

Compatibilidad con bases de datos de ASM de Oracle RAC sin ASMLib

Si utiliza bases de datos Oracle RAC, los nodos RAC deben actualizarse con el archivo

initasmdisks cada vez que se realice una operación en el nodo RAC maestro.

Si no se requiere autenticación para iniciar sesión en los nodos RAC desde el nodo maestro, la asmmain.sh realiza una copia segura (SCP) de inimasmdisks en todos los nodos RAC. El archivo initasmdisks del nodo maestro se llamará cada vez que se produzca la restauración, y la secuencia de comandos asmmain.sh se puede actualizar para invocar la misma secuencia de comandos en todos los nodos RAC.

El archivo /etc/initasmdisks creado que debe ejecutarse desde una de las secuencias de comandos de inicio o desde una secuencia de comandos recientemente definida en rc3.d. El archivo /etc/initasmdisks debe ejecutarse siempre antes de que se inicie el servicio oracleha.

Compatibilidad con bases de datos ASM de Oracle 10g sin ASMLib

Si utiliza Oracle 10g, el comando asmcmd no está disponible para enumerar discos. Puede utilizar la consulta sql para obtener la lista de discos.

La secuencia de comandos disk_list.sql se incluye en las secuencias de comandos existentes proporcionadas en el directorio examples para admitir consultas sql. Al ejecutar el script theasmquerydisk.sh, el script disk_list.sql debe ejecutarse manualmente. Las líneas del script de ejemplo se añaden con comentarios en el archivo asmquerydisk.shl. Este archivo se puede colocar en la ubicación /home/grid u otra ubicación que desee.

Secuencias de comandos de ejemplo para admitir bases de datos ASM sin ASMLib

Los scripts de ejemplo están disponibles en el directorio plugins/examples/noasmlib del directorio de instalación de SnapManager para Oracle.

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$asm_disk;
exit
-bash-4.1$
```

Requisitos para usar bases de datos con NFS y SnapManager

Debe conocer los requisitos para usar las bases de datos con sistema de archivos de red (NFS) y SnapManager. Las recomendaciones incluyen ejecutarse como raíz, caché de atributos y enlaces simbólicos.

- Debe ejecutar SnapManager como raíz; SnapManager debe poder acceder a los sistemas de archivos que contienen archivos de datos, archivos de control, registros de recuperación en línea, registros de archivos y el origen de la base de datos.

  Establezca una de las siguientes opciones de exportación NFS para garantizar que root pueda acceder a los sistemas de archivos:

  - raíz=nombre de host
  - rw=nombre de host, anon=0
- Debe deshabilitar el almacenamiento en caché de atributos para todos los volúmenes que contienen archivos de datos de base de datos, archivos de control, registros de recuperación y archivos, así como el inicio de la base de datos.

  Exporte los volúmenes con las opciones noac (para Solaris y AIX) o actimeo=0 (para Linux).

- Debe vincular los archivos de datos de la base de datos del almacenamiento local a NFS para admitir enlaces simbólicos solamente en el nivel de punto de montaje.

Ejemplos de distribuciones de volúmenes de base de datos

Puede consultar ejemplos de diseños de volumen de base de datos para obtener ayuda en la configuración de la base de datos.

Bases de datos de instancia única

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_sid	Sí	Apagado
Archivos de datos temporales	oratemp_sid	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_sid (multiplexado) Oralog02_sid (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Sí	Apagado

Bases de datos de Real Application Clusters (RAC)

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_dbname	Sí	Apagado
Archivos de datos temporales	oratemp_dbname	Sí	Apagado

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Archivos de control	Oracntrl01_dbname (Multiplexado) Oracntrl02_dbname (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Sí	Apagado
Registros de archivo	oraarch_dbname	Sí	Apagado
Archivos de cluster	oracrs_clustername	Sí	Encendido

Instancia única de una base de datos de Automatic Storage Management (ASM)

Tipos de archivo	Nombres de volúmenes	Nombres de LUN	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	nombre_host de orabin	Sí	Encendido
Archivos de datos	oradata_sid	oradata_sidlun	Sí	Apagado
Archivos de datos temporales	oratemp_sid	OraTemp_sidlun	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Oracntrl01_sidlun (Multiplexado) Oracntrl02_sidlun (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Oralog01_dbnamelun (multiplexado) Oralog02_dbnamelun (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Oraarch_sidlun	Sí	Apagado

Bases de datos RAC ASM

Tipos de archivo	Nombres de volúmenes	Nombres de LUN	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	nombre_host de orabin	Sí	Encendido
Archivos de datos	oradata_sid	oradata_sidlun	Sí	Apagado
Archivos de datos temporales	oratemp_sid	OraTemp_sidlun	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Oracntrl01_sidlun (Multiplexado) Oracntrl02_sidlun (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Oralog01_dbnamelun (multiplexado) Oralog02_dbnamelun (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Oraarch_sidlun	Sí	Apagado
Archivos de cluster	oracrs_clustername	oracrs_clusternamelun	Sí	Encendido

Limitaciones al trabajar con SnapManager

Debe conocer las situaciones y las limitaciones que pueden afectar a su entorno.

Limitaciones relacionadas con diseños y plataformas de bases de datos

- SnapManager admite archivos de control en un sistema de archivos o en un grupo de discos ASM y no admite archivos de control en dispositivos RAW.
- SnapManager funciona en un entorno de cluster Microsoft (MSCS), pero no reconoce el estado de la configuración MSCS (activo o pasivo) y no transfiere la administración activa de un repositorio a un servidor en espera en un clúster MSCS.
- En Red Hat Enterprise Linux (RHEL) y Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 y 5.3 El sistema de archivos ext3 no es compatible al poner en marcha Oracle en dispositivos sin formato mediante multivía dinámica (DMP) en un entorno de I/o de red multivía (MPIO).

  Este problema se observa en SnapManager solo cuando se utiliza SnapDrive 4.1 para UNIX o versiones anteriores.

- SnapManager en RHEL no admite particiones de discos mediante la utilidad **parted**.

Esto es un problema con la utilidad RHEL **parted**.

- En una configuración de RAC, cuando se actualiza un nombre de perfil desde el nodo RAC A, el archivo de programación del perfil se actualiza sólo para el nodo RAC A.

  El archivo de programación para el mismo perfil en el nodo B de RAC no se actualiza y contiene la información de programación anterior. Cuando se activa un backup programado en el nodo B, se produce un error en la operación de backup programada, ya que el nodo B contiene el archivo de programación anterior. Sin embargo, la operación de copia de seguridad programada se realiza correctamente desde el nodo A, en el que se cambia el nombre del perfil. Puede reiniciar el servidor SnapManager para recibir el archivo de programación más reciente para el perfil en el nodo B.

- La base de datos del repositorio puede existir en un host al que se puede acceder mediante más de una dirección IP.

  Si para acceder al repositorio se utiliza más de una dirección IP, se crea el archivo de programación para cada una de las direcciones IP. Si se crea la copia de seguridad de la programación para un perfil (por ejemplo, perfil A) bajo una de las direcciones IP (por ejemplo, IP1), se actualizará el archivo de planificación para sólo esa dirección IP. Si se accede al perfil A desde otra dirección IP (por ejemplo, IP2), la copia de seguridad programada no aparece porque el archivo de programación de IP2 no tiene una entrada para la programación que se creó en IP1.

  Puede esperar a que la programación se active desde esa dirección IP y el archivo de programación que se actualizará o puede reiniciar el servidor.

Limitaciones relacionadas con la configuración de SnapManager

- SnapManager se puede configurar para catalogar backups de bases de datos con RMAN.

  Si se utiliza un catálogo de recuperación de RMAN, el catálogo de recuperación debe estar en una base de datos diferente a la base de datos de la que se realiza el backup.

- SnapDrive para UNIX admite más de un tipo de sistema de archivos y administrador de volúmenes en determinadas plataformas.

  El sistema de archivos y el gestor de volúmenes utilizados para los archivos de la base de datos deben especificarse en el archivo de configuración de SnapDrive como el sistema de archivos predeterminado y el gestor de volúmenes.

- SnapManager admite bases de datos en sistemas de almacenamiento de MultiStore con los siguientes requisitos:
  - Debe configurar SnapDrive para establecer contraseñas para los sistemas de almacenamiento MultiStore.
  - SnapDrive no puede crear una copia snapshot de una LUN o un archivo que reside en un qtree de un sistema de almacenamiento de MultiStore si el volumen subyacente no está en el mismo sistema de almacenamiento de MultiStore.
- SnapManager no admite el acceso a dos servidores SnapManager que se ejecutan en puertos diferentes desde un único cliente (tanto desde la CLI como desde la GUI).

  Los números de puerto deben ser los mismos en los hosts remotos y destino.

- Todas las LUN de un volumen deben estar a nivel de volumen o dentro de qtrees, pero no ambos.

Esto se debe a que, si los datos residen en los qtrees y se monta el volumen, los datos que hay dentro de los qtrees no están protegidos.

- Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

  Es necesario verificar que la base de datos del repositorio esté en ejecución cuando se realiza cualquier operación de SnapManager.

- SnapManager no es compatible con la movilidad de particiones activas (LPM) ni con la movilidad de aplicaciones activas (LAM).
- SnapManager no es compatible con Oracle Wallet Manager ni con el cifrado de datos transparente (TDE).
- SnapManager no admite configuraciones MetroCluster en entornos de asignación de dispositivos sin formato (RDM), ya que las configuraciones de MetroCluster aún deben ser compatibles con Virtual Storage Console (VSC).

Limitaciones relacionadas con la gestión de perfiles

- Si actualiza el perfil para separar los backups de los registros de archivos, no se puede realizar una operación de reversión en el host.
- Si activa un perfil desde la GUI para crear copias de seguridad de registros de archivo y después intenta actualizar el perfil mediante la ventana actualización de perfiles múltiples o la ventana actualización de perfiles, no puede modificar dicho perfil para crear una copia de seguridad completa.
- Si actualiza varios perfiles en la ventana actualización de varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** se desactiva.
- Si actualiza varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** de la ventana actualización de perfiles múltiples está desactivada.
- Si cambia el nombre del perfil, no puede revertir el host.

Limitaciones relacionadas con las operaciones de actualización o reversión

- Si intenta instalar una versión anterior de SnapManager para un host sin realizar la operación de reversión en el host en el repositorio, es posible que no pueda realizar lo siguiente:
  - Ver los perfiles que se crearon en versiones anteriores o posteriores de SnapManager para el host.
  - Acceda a los backups o clones que se crearon en las versiones anteriores o posteriores de SnapManager.
  - Realice operaciones de reversión o actualización en el host.
- Después de separar los perfiles para crear backups de registro de archivos, no se puede ejecutar una operación de reversión en el repositorio de host relacionado.

Limitaciones relacionadas con las operaciones de copia de seguridad

- Se puede producir un error en la creación de backups si se ejecutan operaciones de SnapManager simultáneamente en el mismo host en una base de datos de ASM diferente.
- Durante la recuperación, si el backup ya está montado, SnapManager no volverá a montar el backup y utiliza el backup ya montado.

  Si el backup está montado por un usuario diferente y no tiene acceso al backup montado anteriormente, el

otro usuario debe proporcionarle el permiso.

Todos los archivos de registro de archivos tienen permiso de lectura para los usuarios asignados a un grupo; es posible que no tenga el permiso de acceso al archivo de registro de archivos, si el backup se monta por un grupo de usuarios diferente. Los usuarios pueden otorgar permiso a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la operación de restauración o recuperación.

- SnapManager establece el estado de backup como «PROTEGIDO», incluso cuando una de las copias Snapshot del backup de la base de datos se transfiere al sistema de almacenamiento secundario.
- Puede utilizar el archivo de especificación de tareas para la copia de seguridad programada sólo desde SnapManager 3.2 o posterior.
- Cuando se ejecuta una operación de backup o clonado simultáneamente en las bases de datos de RAC 10gR2 y 11gR2 en ASM, se produce un error en una de las operaciones de creación de clonado o backup.

  Este error se debe a una limitación conocida de Oracle.

- La integración de SnapManager con Protection Manager permite realizar el backup de varios volúmenes en el almacenamiento principal a un único volumen en el almacenamiento secundario para SnapVault y SnapMirror para qtrees.

  No se admite el ajuste de tamaño dinámico de volúmenes secundarios. En la Guía de administración de Provisioning Manager y Protection Manager para usar con DataFabric Manager Server 3.8 encontrará más información al respecto.

- SnapManager no admite copias vault de backups con el script de posprocesamiento.
- Si la base de datos del repositorio apunta a más de una dirección IP y cada dirección IP tiene un nombre de host diferente, la operación de programación de backup se realiza correctamente para una dirección IP, pero falla para la otra dirección IP.
- Después de actualizar a SnapManager 3.4 o una versión posterior, no se podrán actualizar los backups programados con scripts de posprocesamiento que utilicen SnapManager 3.3.1.

  Debe eliminar la programación existente y crear una nueva.

Limitaciones relacionadas con las operaciones de restauración

- Cuando se utiliza un método indirecto para realizar una operación de restauración y los archivos de registro de archivos necesarios para la recuperación solo están disponibles en backups desde el sistema de almacenamiento secundario, SnapManager no logra recuperar la base de datos.

  Esto se debe a que SnapManager no puede montar el backup de los archivos de registro de archivos desde el sistema de almacenamiento secundario.

- Cuando SnapManager realiza una operación de restauración de volúmenes, no se purgan las copias de backup de registros de archivos que se realizan una vez restaurado el backup correspondiente.

  Cuando en el mismo volumen existen los archivos de datos y el destino del archivo de registro de archivos, es posible restaurar los archivos de datos mediante una operación de restauración de volumen si no hay archivos de registro de archivos disponibles en el destino del archivo de registro de archivos. En este caso, se pierden las copias snapshot del registro de archivos que se crean después de la copia de seguridad de los archivos de datos.

  No debe eliminar todos los archivos de registro de archivos del destino del registro de archivos.

- En un entorno ASM, si los archivos de registro de clúster de Oracle (OCR) y de disco de votación coexisten en un grupo de discos que tiene archivos de datos, la operación de vista previa de restauración rápida muestra la estructura de directorio incorrecta para el disco de OCR y de votación.

Limitaciones relacionadas con las operaciones de clonación

- No se puede ver ningún valor numérico entre 0 y 100 en cuanto al progreso de la operación de división de clones debido a la velocidad con la que se detectan y procesan los inodos el sistema de almacenamiento que contiene el volumen flexible.
- SnapManager no admite recibir correos electrónicos solo para las operaciones de división de clones correctamente.
- SnapManager solo admite la división de un FlexClone.
- Se produce un error en la clonado del backup de la base de datos en línea de la base de datos RAC donde se usa la ubicación del archivo de registro de archivos externo debido a un error en la recuperación.

  Se produce un error en la clonado porque Oracle no encuentra y aplica los archivos de registro de archivos para la recuperación desde la ubicación del registro de archivos externo. Esta es una limitación de Oracle. Para obtener más información, consulte el ID de error de Oracle: 13528007. Oracle no aplica el registro de archivo desde la ubicación no predeterminada en la "Sitio de soporte de Oracle". Debe tener un nombre de usuario y una contraseña de Oracle metalink válidos.

- SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.
- Si los espacios de tablas temporales se encuentran en una ubicación diferente a la ubicación de los archivos de datos, una operación de clonado crea los espacios de tabla en la ubicación de los archivos de datos.

  Sin embargo, si los espacios de tablas temporales son Oracle Managed Files (OMF) ubicados en una ubicación diferente a la ubicación de los archivos de datos, la operación de clonado no crea los espacios de tablas en la ubicación de los archivos de datos. SnapManager no gestiona los OMF.

- SnapManager no puede clonar una base de datos de RAC si selecciona la opción -resetlogs.

Limitaciones relacionadas con archivos de registro de archivos y copias de seguridad

- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino de área de recuperación flash.
- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino en espera.
- Los backups de registros de archivos se retienen en función de la duración de la retención y la clase de retención por horas predeterminada.

  Cuando la clase de retención de backup de registros de archivos se modifica mediante la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager, la clase de retención modificada no se considera para el backup porque los backups de registros de archivo se retienen en función de la duración de la retención.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, el backup de registros de archivos no incluye los archivos de registro de archivos más antiguos que el archivo de registro de archivos faltante.

  Si falta el archivo de registro de archivos más reciente, la operación de backup del registro de archivos falla.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.
- SnapManager consolida los backups de registros de archivos incluso cuando se eliminan los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados.

Limitaciones relacionadas con el cambio del nombre de host de la base de datos de destino

No se admiten las siguientes operaciones de SnapManager cuando se cambia el nombre de host de la base de datos de destino:

- Cambiar el nombre de host de la base de datos de destino desde la interfaz gráfica de usuario de SnapManager.
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil.
- Al mismo tiempo, se actualizan varios perfiles para un nuevo nombre de host de base de datos de destino.
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager.

Limitaciones relacionadas con la CLI o GUI de SnapManager

- Los comandos de la CLI de SnapManager para la operación de creación de perfiles que se generan desde la interfaz gráfica de usuario de SnapManager no tienen opciones de configuración del historial.

  No se puede utilizar el comando profile create para configurar las opciones de retención del historial desde la interfaz de línea de comandos de SnapManager.

- SnapManager no muestra la GUI en Mozilla Firefox cuando no hay Java Runtime Environment (JRE) disponible en el cliente UNIX.
- Al actualizar el nombre de host de la base de datos de destino mediante la interfaz de línea de comandos de SnapManager, si hay una o más sesiones abiertas de la interfaz gráfica de usuario de SnapManager, todas las sesiones abiertas de la interfaz gráfica de usuario de SnapManager no pueden responder.

Limitaciones relacionadas con SnapMirror y SnapVault

- El script de posprocesamiento de SnapVault no es compatible si se utiliza Data ONTAP en 7-Mode.
- Si utiliza ONTAP, no puede ejecutar SnapRestore (VBSR) basada en volúmenes en los backups creados en los volúmenes que tienen relaciones de SnapMirror establecidas.

  Esto se debe a una limitación de ONTAP, que no permite romper la relación al realizar una VBSR. Sin embargo, se puede ejecutar un VBSR en el backup último o más reciente creado solo cuando los volúmenes tienen relaciones de SnapVault establecidas.

- Si utiliza Data ONTAP operando en 7-Mode y desea ejecutar un VBSR en los backups creados en los volúmenes que tienen relaciones de SnapMirror establecidas, puede establecer la opción override-vbsr-snapmirror-check en ON en SnapDrive para UNIX.

  La documentación de SnapDrive contiene más información al respecto.

- En algunos casos, no se puede eliminar el último backup asociado con la primera copia Snapshot cuando se ha establecido una relación de SnapVault en el volumen.

  Puede eliminar el backup solo cuando se rompa la relación. Este problema se debe a una restricción de la

ONTAP con copias Snapshot base. En una relación de SnapMirror, la copia de Snapshot básica se crea mediante el motor de SnapMirror y, en una relación de SnapVault, la copia de Snapshot base es el backup creado mediante SnapManager. Para cada actualización, la copia snapshot básica señala el backup más reciente creado mediante SnapManager.

Limitaciones relacionadas con las bases de datos en espera de Data Guard

- SnapManager no admite bases de datos lógicas en espera de Data Guard.
- SnapManager no admite bases de datos en espera de Active Data Guard.
- SnapManager no permite realizar backups en línea de bases de datos Data Guard en espera.
- SnapManager no permite backups parciales de bases de datos en espera de Data Guard.
- SnapManager no permite la restauración de bases de datos Data Guard en espera.
- SnapManager no permite eliminar archivos de registro de archivos para bases de datos en espera de Data Guard.
- SnapManager no admite Data Guard Broker.

Información relacionada

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Limitaciones de SnapManager para Clustered Data ONTAP

Debe conocer las limitaciones de algunas funcionalidades y operaciones de SnapManager si utiliza Clustered Data ONTAP.

Las siguientes funcionalidades no son compatibles si utiliza SnapManager en Clustered Data ONTAP:

- Funcionalidades de protección de datos si SnapManager se integra con Unified Manager de OnCommand
- Una base de datos en la que una LUN pertenece a un sistema que ejecuta Data ONTAP en 7-Mode y la otra LUN pertenece a un sistema que ejecuta Clustered Data ONTAP
- SnapManager para Oracle no admite la migración de un Vserver, que no es compatible con Clustered Data ONTAP
- SnapManager para Oracle no admite la funcionalidad Clustered Data ONTAP 8.2.1 para especificar diferentes políticas de exportación para volúmenes y qtrees

Limitaciones relacionadas con Oracle Database

Antes de empezar a trabajar con SnapManager, debe conocer las limitaciones relacionadas con la base de datos de Oracle.

Estas limitaciones son las siguientes:

- SnapManager es compatible con las versiones 10gR2, 11gR1, 11gR2 y 12*c*_, pero no es compatible con Oracle 10gR1 como repositorio o base de datos de destino.
- SnapManager no admite el uso de una dirección IP DE EXPLORACIÓN en lugar de un nombre de host.

  SCAN IP es una nueva función de Oracle 11gR2.

- SnapManager no es compatible con Oracle Cluster File System (OCFS).

- Oracle 11g en un entorno de NFS directo (dNFS) permite configuraciones de punto de montaje adicionales en el archivo Naranfstab, como varias rutas para el equilibrio de carga.

  SnapManager no modifica el archivo anorfstab. Debe agregar manualmente todas las propiedades adicionales que desee que utilice la base de datos clonada en el archivo oranfstab.

- La compatibilidad con bases de datos Oracle 9i se usa en SnapManager 3.2.
- La compatibilidad con la base de datos Oracle 10gR2 (anterior a 10.2.0.5) queda obsoleta en SnapManager 3.3.1.

> Identifique las distintas versiones de las bases de datos de Oracle que se admiten en la matriz de interoperabilidad.

Información relacionada

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Versiones obsoletas de la base de datos Oracle

SnapManager 3.2 o posterior no admite la base de datos Oracle 9i, y la base de datos Oracle 10gR2 (anterior a 10.2.0.4) no es compatible con SnapManager 3.3.1 o posterior.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o posterior, no puede crear perfiles nuevos; se muestra un mensaje de advertencia.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o una versión posterior, debe realizar una de las siguientes acciones:

- Actualice las bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) a bases de datos de Oracle 10gR2 (10.2.0.5), 11gR1 o 11gR2 y, a continuación, actualice a SnapManager 3.2 o 3.3.

  Si va a actualizar a Oracle 12*c*, debe actualizar a SnapManager 3.3.1 o posterior.

  > La base de datos Oracle 12*c* sólo se admite desde SnapManager 3.3.1.

- Gestión de las bases de datos Oracle 9i mediante una versión de revisión de SnapManager 3.1.

  Puede utilizar SnapManager 3.2 o 3.3 si desea gestionar bases de datos Oracle 10gR2, 11gR1 o 11gR2 y utilizar SnapManager 3.3.1 o posterior si desea gestionar bases de datos Oracle 12*c* junto con otras bases de datos compatibles.

Restricciones en la gestión de volúmenes

SnapManager tiene ciertas restricciones de gestión de volúmenes que pueden afectar al entorno.

Es posible tener varios grupos de discos para una base de datos; sin embargo, las siguientes limitaciones se aplican a todos los grupos de discos de una base de datos determinada:

- Los grupos de discos de la base de datos solo pueden gestionarse un gestor de volúmenes.
- Los dispositivos sin formato respaldados por un gestor de volúmenes lógicos no son compatibles con la protección de los datos de Oracle.

El almacenamiento de dispositivos sin procesar y los grupos de discos de gestión automática de almacenamiento (ASM) se deben aprovisionar directamente en los dispositivos físicos. En algunos casos, se requiere la partición.

- Un entorno Linux sin gestión de volúmenes lógicos requiere una partición.

Crear backups usando copias de Snapshot

SnapManager permite crear backups en el almacenamiento primario (local) y en el almacenamiento secundario (remoto) mediante políticas de protección o scripts postprocesamiento.

Los backups que se crean como copias Snapshot son copias virtuales de la base de datos y se almacenan en el mismo medio físico que la base de datos. Por consiguiente, la operación de backup requiere menos tiempo y mucho menos espacio que los backups completos de disco a disco. SnapManager permite realizar el backup de los siguientes elementos:

- Todos los archivos de datos, los archivos de registro de archivo y los archivos de control
- Los archivos de datos o espacios de tablas seleccionados, todos los archivos de registro de archivo y los archivos de control

SnapManager 3.2 o posterior le permite realizar, opcionalmente, el backup de lo siguiente:

- Todos los archivos de datos y los archivos de control
- Los archivos de datos o tablespaces seleccionados junto con los archivos de control
- Archivos de registro de archivo

> Los archivos de datos, los archivos de registro de archivos y los archivos de control pueden ubicarse en diferentes sistemas de almacenamiento, volúmenes de sistema de almacenamiento y números de unidad lógica (LUN). También se puede usar SnapManager para realizar backup de una base de datos cuando hay varias bases de datos en el mismo volumen o LUN.

Por qué debe prune los archivos de registro de archivos

SnapManager para Oracle permite eliminar archivos de registro de archivos del sistema de archivos activo de del que ya se ha realizado un backup.

Eliminar permite a SnapManager crear backups de diferentes archivos de registro de archivos. Eliminar, junto con la política de retención de backups, libera espacio en los registros de archivos cuando se purgan los backups.

> No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos. Si especifica la ubicación del registro de archivos en el área de recuperación flash, debe asegurarse de especificar también la ubicación del registro de archivos en el parámetro archive_log_dest.

Consolidación de registros de archivo

SnapManager (3.2 o posterior) para Oracle consolida los backups de registros de

archivos a fin de mantener una cantidad mínima de backups para los archivos de registro de archivos. SnapManager para Oracle identifica y libera los backups que contienen archivos de registros de archivos que son subconjuntos de otros backups.

Restauración total o parcial de bases de datos

SnapManager proporciona la flexibilidad necesaria para restaurar bases de datos completas, espacios de tablas específicos, archivos, archivos de control o una combinación de estas entidades. SnapManager le permite restaurar datos mediante un procesador de restauración basado en archivos un proceso de restauración más rápido y basado en volúmenes. Los administradores de bases de datos pueden seleccionar el proceso que desean utilizar o dejar que SnapManager decida qué proceso es apropiado.

SnapManager permite a los administradores de bases de datos obtener una vista previa de las operaciones de restauración. La función de vista previa permite a los administradores de bases de datos ver cada operación de restauración archivo por archivo.

Los administradores de bases de datos pueden especificar el nivel en el que SnapManager restaura y recupera la información cuando se ejecutan operaciones de restauración. Por ejemplo, los administradores de bases de datos pueden restaurar y recuperar datos en momentos específicos. El punto de restauración puede ser una fecha y hora, o un número de cambio de sistema (SCN) de Oracle.

Los administradores de bases de datos pueden usar SnapManager para restaurar la base de datos y usar otra herramienta para recuperar la información. Los administradores de bases de datos no tienen que usar SnapManager para ambas operaciones.

SnapManager (3.2 o posterior) permite restaurar y recuperar backups de bases de datos de forma automática sin intervención del administrador de base de datos. Es posible usar SnapManager para crear backups de registros de archivo, y luego usarlos para restaurar y recuperar los backups de bases de datos. Aunque los archivos de registro de archivo del backup se gestionen en una ubicación de un registro de archivo externo, puede especificar esa ubicación externa para que los registros de archivos puedan ayudar a recuperar la base de datos restaurada.

Comprobar el estado del backup

SnapManager puede confirmar la integridad del backup mediante las operaciones estándar de verificación de backup de Oracle.

Los administradores de bases de datos pueden realizar la verificación como parte de la operación de backup o al mismo tiempo. Los administradores de bases de datos pueden configurar la operación de verificación para que se produzca durante un tiempo de pico de actividad cuando la carga en los servidores host es menor o durante un período de mantenimiento programado.

Clones de backups de bases de datos

SnapManager utiliza la tecnología FlexClone para crear un clon modificable de un backup de base de datos con un uso eficiente del espacio. Es posible modificar un clon sin cambiar el origen de backup.

Quizás sería conveniente clonar bases de datos para permitir pruebas o actualizaciones en entornos no

productivos. Es posible clonar una base de datos que reside en el almacenamiento secundario primor. Puede ubicarse un clon en el mismo host o en otro que la base de datos.

La tecnología FlexClone permite a SnapManager utilizar copias snapshot de la base de datos para evitar crear una copia física completa de disco a disco. Las copias Snapshot requieren menos tiempo de creación y ocupan mucho menos espacio que las copias físicas.

Consulte la documentación de Data ONTAP para obtener más información sobre la tecnología FlexClone.

Información relacionada

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

Realizar un seguimiento de los detalles y generar informes

SnapManager reduce el nivel de detalle que los administradores de las bases de datos necesitan para realizar un seguimiento del estado de las diferentes operaciones mediante la oferta de métodos para supervisar las operaciones desde una única interfaz.

Una vez que los administradores especifican qué bases de datos deben realizarse backups, SnapManager identifica automáticamente los archivos de la base de datos para el backup. SnapManager muestra información sobre repositorios, hosts, perfiles, backups y clones. Puede supervisar las operaciones en hosts o bases de datos específicos.también puede identificar los backups protegidos y determinar si los backups están en proceso o si están programados para producirse.

Qué repositorios son

SnapManager organiza la información en perfiles, que a continuación se asocian con repositorios. Los perfiles contienen información acerca de la base de datos que se está gestionando, mientras que el repositorio contiene datos acerca de las operaciones que se realizan en los perfiles.

El repositorio registra el momento en que se realizó un backup, qué archivos se hicieron de backup y si se creó un clon a partir del backup. Cuando los administradores de bases de datos restauran una base de datos o recuperan una parte del mismo, SnapManager consulta el repositorio para determinar qué se ha realizado un backup.

Como el repositorio almacena los nombres de las copias Snapshot de la base de datos creadas durante las operaciones de backup, la base de datos del repositorio no puede existir en la misma base de datos y tampoco puede formar parte de la misma base de datos de la que se realiza el backup de SnapManager. Debe tener al menos dos bases de datos (la base de datos del repositorio de SnapManager y la base de datos de destino que gestiona SnapManager) en funcionamiento cuando se ejecutan operaciones de SnapManager.

Si intenta abrir la interfaz gráfica de usuario (GUI) cuando la base de datos del repositorio está inactiva, se registra el siguiente mensaje de error en el archivo sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: No se han producido más datos para leer desde el socket. Además, se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva. Para obtener más información acerca de los diferentes mensajes de error, consulte *solución de problemas conocidos*.

Es posible usar cualquier nombre de host, nombre de servicio o nombre de usuario válido para realizar operaciones. Para que un repositorio admita operaciones SnapManager, el nombre de usuario y el nombre de servicio del repositorio sólo deben contener los siguientes caracteres: Caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-), guión bajo (_) y punto (.).

El puerto de repositorio puede ser cualquier número de puerto válido y el nombre de host del repositorio puede ser cualquier nombre de host válido. El nombre de host debe estar formado por caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-) y punto (.), pero no un guión bajo (_).

El repositorio debe crearse en una base de datos de Oracle. La base de datos que utiliza SnapManager debe configurarse de acuerdo con los procedimientos de Oracle para la configuración de la base de datos.

Un único repositorio puede contener información acerca de varios perfiles; sin embargo, cada base de datos normalmente se asocia a un único perfil. Puede tener varios repositorios, donde cada repositorio contiene varios perfiles.

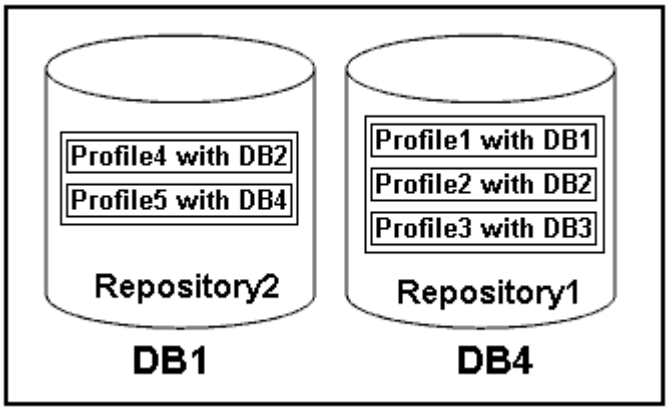
Qué perfiles son

SnapManager utiliza perfiles para almacenar la información necesaria para realizar operaciones en una base de datos determinada. Un perfil contiene información sobre la base de datos, incluidas sus credenciales, backups y clones. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos.

Un perfil sólo puede hacer referencia a una base de datos. Más de un perfil puede hacer referencia a la misma base de datos. No es posible acceder a los backups creados con un perfil desde otro perfil, aunque ambos perfiles hagan referencia a la misma base de datos.

La información del perfil se almacena en un repositorio. El repositorio contiene información de perfil de la base de datos e información sobre las copias de Snapshot que sirven como backup de base de datos. Las copias Snapshot reales se almacenan en el sistema de almacenamiento. Los nombres de las copias Snapshot se almacenan en el repositorio que contiene el perfil de esa base de datos. Cuando se realiza una operación en una base de datos, debe seleccionar el perfil en el repositorio.

La siguiente figura muestra cómo los repositorios pueden contener varios perfiles, pero también que cada perfil puede definir sólo una base de datos:



En el ejemplo anterior, deleteRepository2 se encuentra en la base de datos DB1 y deleteRepository1 en la base de datos DB4.

Cada perfil contiene las credenciales de la base de datos asociada al perfil. Las credenciales permiten que SnapManager se conecte a la base de datos y trabaje con ella. Las credenciales almacenadas incluyen el nombre de usuario y las parejas de contraseñas para acceder al host, al repositorio, a la base de datos y a la información de conexión necesaria si utiliza Oracle Recovery Manager (RMAN).

No se puede acceder a un backup que se creó con un perfil de otro perfil, incluso si los dos perfiles están asociados con la misma base de datos. SnapManager coloca un bloqueo en la base de datos para evitar que se realicen dos operaciones incompatibles a la vez.

Perfil para crear copias de seguridad completas y parciales

Puede crear perfiles para realizar copias de seguridad completas o parciales.

Los perfiles que se especifican para crear las copias de seguridad completas y parciales contienen tanto los archivos de datos como los archivos de registro de archivos. SnapManager no permite que dichos perfiles separen los backups de registros de archivo de los backups del archivo de datos. Los backups completos y parciales se retienen en función de las políticas de retención de backup existentes y se protegen de acuerdo con las políticas de protección existentes. Puede programar copias de seguridad completas y parciales en función del tiempo y la frecuencia que mejor le convenga.

Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad de sólo registro de archivos

SnapManager (3.2 o posterior) permite crear perfiles para realizar backups de los archivos de registro de archivos independientemente de los archivos de datos. Después de usar el perfil para separar los tipos de backup, es posible crear backups de solo los archivos de datos o backups de solo registros de archivos de la base de datos. También es posible crear un backup que contenga los archivos de datos y los archivos de registro de archivos juntos.

La política de retención se aplica a todos los backups de la base de datos cuando no están separados los backups de registros de archivos. Después de separar los backups de registros de archivos, SnapManager permite especificar diferentes duraciones de retención y políticas de protección para los backups de registros de archivos.

Política de retención

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Una copia de seguridad caduca cuando su antigüedad supera el período de retención establecido para su clase de retención y la cantidad de backups supera el número de retención. Por ejemplo, si el número de backup es 15 (lo que significa que SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups más antiguos, correctos y elegibles caducan.

Duración de la retención del registro de archivo

Una vez separados los backups de los registros de archivos, se retienen en función de la duración de la retención de los registros de archivos. Los backups de registros de archivo que se realizan con los backups de archivos de datos siempre se conservan junto con estos backups de archivos de datos, independientemente de la duración de la retención de registros de archivo.

Información relacionada

Gestionar perfiles para backups eficientes

Qué son los estados de operación de SnapManager

Las operaciones de SnapManager (backup, restauración y clonado) pueden estar en diferentes estados y cada estado indica el progreso de la operación.

Estado de la operación	Descripción
Correcto	La operación se ha completado correctamente.
Ejecutando	La operación se inició, pero no ha finalizado. Por ejemplo, se programa que un backup, que tarda dos minutos, se lleve a cabo a las 11:00. Al ver la ficha **Programación** a las 11:01 a.m., la operación aparece como en ejecución.
No se ha encontrado ninguna operación	La programación no se ha ejecutado o se ha eliminado la última copia de seguridad ejecutada.
Error	Error en la operación. SnapManager ha ejecutado automáticamente el proceso de anulación y ha limpiado la operación. **Nota:** puede dividir el clon que se crea. Cuando se detiene la operación de división de clones que se inició y la operación se detiene correctamente, el estado de la operación de división de clones muestra como error.

Eventos recuperables e irrecuperables

Un evento SnapManager recuperable tiene los siguientes problemas:

- La base de datos no se almacena en un sistema de almacenamiento que ejecuta Data ONTAP.
- Se configuró una base de datos de Automatic Storage Management (ASM), pero no se está ejecutando la instancia de ASM.
- SnapDrive para UNIX no está instalado o no puede acceder al sistema de almacenamiento.
- SnapManager no puede crear una copia Snapshot o aprovisionar almacenamiento si el volumen no tiene espacio, se alcanzó el número máximo de copias Snapshot o se produce una excepción no prevista.

Cuando se produce un evento recuperable, SnapManager realiza un proceso de anulación e intenta devolver el host, la base de datos y el sistema de almacenamiento al estado inicial. Si el proceso de anulación falla, SnapManager trata el incidente como un evento irrecuperable.

Un evento irrecuperable (fuera de banda) se produce cuando se produce cualquiera de los siguientes acontecimientos:

- Se produce un problema con el sistema, como cuando se produce un error en un host.
- Se ha detenido el proceso SnapManager.
- Se produce un error en una operación de anulación en banda cuando el sistema de almacenamiento falla, el número de unidad lógica (LUN) o el volumen de almacenamiento están sin conexión o la red falla.

Cuando se produce un evento irrecuperable, SnapManager realiza un proceso de cancelación inmediatamente. Es posible que el host, la base de datos y el sistema de almacenamiento no regresen a los estados iniciales. Si este es el caso, debe realizar una limpieza después de que la operación SnapManager falle; para ello, elimine la copia snapshot huérfana y elimine el archivo de bloqueo de SnapManager.

Si desea eliminar el archivo de bloqueo SnapManager, desplácese a $ORACLE_HOME en el equipo de destino y elimine el archivo sm_lock_TargetDBName. Después de eliminar el archivo, debe reiniciar SnapManager para Oracle Server.

Cómo mantiene SnapManager la seguridad

Es posible realizar operaciones de SnapManager solo si cuenta con las credenciales adecuadas. La seguridad en SnapManager está regida por la autenticación de usuarios y el control de acceso basado en roles (RBAC). RBAC permite que los administradores de bases de datos restrinjan las operaciones que SnapManager puede realizar en los volúmenes y LUN que contienen los archivos de datos de una base de datos.

Los administradores de bases de datos habilitan el RBAC para SnapManager mediante SnapDrive. A continuación, los administradores de bases de datos asignan permisos a los roles de SnapManager y asignan estos roles a los usuarios en la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) de Operations Manager. Las comprobaciones de permisos de RBAC se realizan en DataFabric Manager Server.

Además del acceso basado en roles, SnapManager mantiene la seguridad mediante la solicitud de autenticación de usuario mediante solicitudes de contraseña o la configuración de credenciales de usuario. Un usuario efectivo se autentica y autoriza con el servidor SnapManager.

Las credenciales de SnapManager y la autenticación de usuario difieren significativamente de SnapManager 3.0:

- En las versiones de SnapManager anteriores a la 3.0, debe establecer una contraseña de servidor arbitraria al instalar SnapManager. Cualquier persona que desee utilizar el servidor SnapManager necesitará la contraseña del servidor SnapManager. La contraseña del servidor SnapManager debería añadirse a las credenciales de usuario mediante el comando smo credential set -host.
- En SnapManager (3.0 y posterior), la contraseña del servidor SnapManager ha sido sustituida por la autenticación individual del sistema operativo (SO) de usuario. Si no ejecuta el cliente desde el mismo servidor que el host, el servidor SnapManager realiza la autenticación con los nombres de usuario y contraseñas del sistema operativo. Si no desea que se le soliciten las contraseñas de sistema operativo, puede guardar los datos en la caché de credenciales de usuario de SnapManager mediante el comando smo credential set -host.

> El comando smo credential set -host recuerda las credenciales cuando la propiedad host.credentials.persists del archivo smo.config está establecida en TRUE.

ejemplo

User1 y User2 comparten un perfil denominado Pro2. User2 no puede realizar una copia de seguridad de Database1 en Host1 sin permiso para acceder a Host1. User1 no puede clonar una base de datos a Host3 sin permiso para acceder a Host3.

En la siguiente tabla se describen los diferentes permisos asignados a los usuarios:

Tipo de permiso	Usuario1	Usuario2
Contraseña del host	Host1, Host2	Host2, Host3
Contraseña de repositorio	Repo. 1	Repo. 1
Contraseña de perfil	Pro1, Pro2	Profeca2

En caso de que User1 y User2 no tengan ningún perfil compartido, supongamos que User1 tiene permisos para los hosts denominados Host1 y Host2 y que User2 tiene permisos para el host denominado Host2. User2 no puede ejecutar ni siquiera los comandos que no son de perfil, como dump y verificación del sistema en Host1.

Acceso e impresión de la Ayuda en línea

La Ayuda en línea proporciona instrucciones para las tareas que puede realizar mediante la interfaz gráfica de usuario de SnapManager. La Ayuda en línea también proporciona descripciones de los campos de las ventanas y asistentes.

1. Ejecute una de las siguientes acciones:
   - En la ventana principal, haga clic en **Ayuda** > **Contenido de la Ayuda**.
   - En cualquier ventana o asistente, haga clic en **Ayuda** para ver la ayuda específica de esa ventana.
2. Utilice **Tabla de contenido** en el panel izquierdo para navegar por los temas.
3. Haga clic en el icono impresora situado en la parte superior de la ventana de ayuda para imprimir temas individuales.

Diseños generales de bases de datos y configuraciones de almacenamiento recomendados

Conocer los diseños generales recomendados de las bases de datos y las configuraciones de almacenamiento puede ayudarle a evitar problemas relacionados con los grupos de discos, los tipos de archivos y los espacios de tablas.

- No incluya archivos de más de un tipo de sistema de archivos SAN o administrador de volúmenes en la base de datos.

  Todos los archivos que conforman una base de datos deben residir en el mismo tipo de sistema de archivos.

- SnapManager requiere un gran tamaño de bloque de 4 KB.
- Incluyen el identificador del sistema de la base de datos en el archivo oratab.

  Incluir una entrada en el archivo oratab de cada base de datos que se gestionará. SnapManager utiliza el archivo oratab para determinar qué directorio raíz de Oracle usar.

- Para registrar backups de SnapManager en Oracle RMAN, debe crear perfiles habilitados para RMAN.

Si desea aprovechar la nueva restauración basada en volúmenes o la restauración de grupos de discos

completos, tenga en cuenta las siguientes directrices relacionadas con los sistemas de archivos y los grupos de discos:

- Varias bases de datos no pueden compartir el mismo grupo de discos de Automatic Storage Management (ASM).
- Un grupo de discos que contiene archivos de datos no puede contener otros tipos de archivos.
- El número de unidad lógica (LUN) para el grupo de discos de archivos de datos debe ser el único objeto del volumen de almacenamiento.

A continuación se muestran algunas directrices para la separación de volúmenes:

- Los archivos de datos de una sola base de datos deben estar en el volumen.
- Debe utilizar volúmenes independientes para cada una de las siguientes clasificaciones de archivos: Archivos binarios de base de datos, archivos de datos, archivos redo log en línea, archivos redo log archivados y archivos de control.
- No es necesario crear un volumen separado para los archivos de base de datos temporales, ya que SnapManager no realiza backups de archivos de base de datos temporales.

Definir el inicio de la base de datos con el archivo oratab

SnapManager utiliza el archivo oratab durante las operaciones para determinar el directorio inicial de la base de datos de Oracle. Una entrada de la base de datos de Oracle debe estar en el archivo oratab para que SnapManager funcione correctamente. El archivo oratab se crea durante la instalación del software de Oracle.

El archivo oratab reside en diferentes ubicaciones según el sistema operativo del host, como se muestra en la siguiente tabla:

Sistema operativo del host	Ubicación del archivo
Linux	/etc/oratab
Solaris	/var/opt/oracle/oratab
IBM AIX	/etc/oratab

El archivo oratab de muestra contiene la siguiente información:

```
+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
```

Después de instalar Oracle, debe asegurarse de que el archivo oratab resida en la ubicación especificada en la tabla anterior. Si el archivo oratab no reside en la ubicación correcta por cada sistema operativo, debe comunicarse con el soporte técnico para obtener ayuda.

Requisitos para usar bases de datos de RAC con SnapManager

Debe conocer las recomendaciones para usar bases de datos de Real Application Clusters (RAC) con SnapManager. Las recomendaciones incluyen números de puerto, contraseñas y modo de autenticación.

- En el modo de autenticación de la base de datos, el listener de cada nodo que interactúa con una instancia de la base de datos RAC debe configurarse para que utilice el mismo número de puerto.

  El listener que interactúa con la instancia de base de datos primaria debe iniciarse antes de iniciar el backup.

- En modo de autenticación del sistema operativo o en un entorno de ASM, se debe instalar y ejecutar el servidor SnapManager en cada nodo del entorno RAC.
- La contraseña de usuario de la base de datos (por ejemplo, para un administrador del sistema o un usuario con el privilegio sysdba) debe ser la misma para todas las instancias de la base de datos Oracle en un entorno RAC.

Requisitos para usar bases de datos de ASM con SnapManager

Debe conocer los requisitos para usar las bases de datos de gestión automática de almacenamiento (ASM) con SnapManager. Conocer estos requisitos puede ayudarle a evitar problemas con ASMLib, particiones y especificaciones de clonación, entre otras cosas.

- SnapManager (3.0.3 o posterior) utiliza el nuevo privilegio sysasm disponible con Oracle 11gR2 en lugar del privilegio sysdba para administrar una instancia de Oracle ASM.

  Si utiliza el privilegio sysdba para ejecutar comandos administrativos en la instancia de ASM, se muestra un mensaje de error. La base de datos utiliza el privilegio sysdba para acceder a los grupos de discos. Si se conecta a la instancia de ASM mediante el privilegio sysasm, tendrá acceso completo a todos los grupos de discos y funciones de administración de Oracle ASM disponibles.

  > Si utiliza Oracle 10gR2 y 11gR1, debe continuar utilizando el privilegio sysdba.

- SnapManager (3.0.3 o posterior) admite la copia de seguridad de bases de datos que se almacenan directamente en grupos de discos ASM cuando el grupo de discos también contiene un volumen de sistema automático de archivos de clúster (ACFS).

  Estos archivos están protegidos indirectamente por SnapManager y pueden restaurarse con el contenido restante de un grupo de discos de ASM, pero SnapManager (3.0.3 o posterior) no admite ACFS.

  > ACFS es una tecnología de gestión del almacenamiento del sistema de archivos escalable y multiplataforma disponible con Oracle 11gR2. ACFS amplía la funcionalidad ASM para admitir archivos de clientes que se mantienen fuera de la base de datos Oracle.

- SnapManager (3.0.3 o posterior) admite la copia de seguridad de archivos almacenados en grupos de discos ASM cuando el grupo de discos también contiene archivos de registro de cluster Oracle (OCR) o archivos de disco de votación; sin embargo, las operaciones de restauración requieren un método más lento, basado en host o de restauración instantánea de archivo parcial (PFSR).

  Es mejor tener discos OCR y de votación en grupos de discos que no contengan archivos de base de

datos.

- Cada disco utilizado para ASM debe contener sólo una partición.
- La partición que aloja los datos de ASM debe estar correctamente alineada para evitar problemas graves de rendimiento.

  Esto implica que la LUN debe ser del tipo correcto y la partición debe tener un desplazamiento que es un múltiplo de 4K bytes.

  Para obtener más información sobre cómo crear particiones alineadas con 4K, consulte el artículo 1010717 de Knowledge base.

- No se especifica la configuración de ASM como parte de la especificación del clon.

  Debe quitar manualmente la información de configuración de ASM en las especificaciones de clonado que se crearon con SnapManager 2.1 antes de actualizar el host a SnapManager (2.2 o posterior).

- SnapManager 3.1, 3.1p1 y 3.2 o posterior admiten ASMLib 2.1.4.
- SnapManager 3.1p4 o posterior admiten ASMLib 2.1.4, 2.1.7 y 2.1.8.

Dispositivos de partición compatibles

Debe conocer los diferentes dispositivos de partición compatibles con SnapManager.

La siguiente tabla proporciona información de partición y cómo se puede activar para diferentes sistemas operativos:

De NetApp	Partición única	Partición múltiple	Dispositivos sin partición	Sistema de archivos o dispositivos RAW
Red Hat Enterprise Linux 5x o 5 veces Oracle Enterprise Linux	Sí	No	No	ext3*
Red Hat Enterprise Linux 6xor 6 veces Oracle Enterprise Linux	Sí	No	No	ext3 o ext4*
SUSE Linux Enterprise Server 11	Sí	No	No	ext3*
SUSE Linux Enterprise Server 10	No	No	Sí	ext3***

De NetApp	Partición única	Partición múltiple	Dispositivos sin partición	Sistema de archivos o dispositivos RAW
Red Hat Enterprise Linux 5x o posterioresor Oracle Enterprise Linux 5 o posterior	Sí	No	Sí	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4or SUSE Linux Enterprise Server 11	Sí	No	Sí	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4 o posteror SUSE Linux Enterprise Server 11	Sí	No	No	ASM sin ASMLib**

Para obtener más información sobre las versiones compatibles del sistema operativo, consulte la matriz de interoperabilidad.

Compatibilidad con ASMLib

SnapManager admite diferentes versiones de ASMLib, aunque hay varios factores que debe tener en cuenta al utilizar SnapManager con ASMLib.

SnapManager admite ASMLib 2.1.4, 2.1.7 y 2.1.8. Todas las operaciones de SnapManager se pueden realizar con ASMLib 2.1.4, 2.1.7 y 2.1.8.

Si actualizó desde ASMLib 2.1.4 a ASM 2.1.7, es posible usar los mismos perfiles y backups creados con ASMLib 2.1.4 para restaurar los backups y crear los clones.

Debe tener en cuenta lo siguiente al utilizar SnapManager con ASMLib:

- SnapManager 3.1 no admite ASMLib 2.1.7.

  SnapManager 3.1p4 o posterior admiten ASMLib 2.1.4, 2.1.7 y 2.1.8.

- Después de realizar una actualización sucesiva desde SnapManager 3.1 a 3.2, las copias de seguridad creadas mediante ASMLib 2.1.7 funcionan únicamente si el repositorio se revierte a SnapManager 3.1 y ASMLib 2.1.7 se degrada a ASMLib 2.1.4.
- Después de realizar una actualización sucesiva desde SnapManager 3.1 a 3.2, las copias de seguridad creadas con ASMLib 2.1.7 no funcionan si el repositorio se revierte a SnapManager 3.1 con ASMLib 2.1.7.

  La reversión se realiza correctamente, pero no se pueden utilizar los perfiles y las copias de seguridad.

Compatibilidad con bases de datos de ASM sin ASMLib

SnapManager admite ASM sin ASMLib, de forma predeterminada. El requisito básico es que se deban particionar los dispositivos que se usan para los grupos de discos ASM.

Cuando ASMLib no está instalado, los permisos de dispositivo relacionados con los grupos de discos de ASM cambian a root:disk cuando se realizan las siguientes operaciones:

- Reinicie el host
- Restaure una base de datos desde el almacenamiento principal mediante SnapRestore (VBSR) basada en volúmenes.
- Restaurar una base de datos desde el almacenamiento secundario

Puede establecer los permisos de dispositivo adecuados asignando true a la variable de configuración oracleasm.support.without.asmlib en smo.conf. Los dispositivos relacionados con los grupos de discos ASM se agregan o eliminan del archivo initasmdisks cada vez que se agregan o eliminan nuevos dispositivos del host. El archivo initasmdisks está ubicado en /etc/initasmdisks.

Por ejemplo, si establece oracleasm.support.without.asmlib=true y, a continuación, realiza un montaje de copia de seguridad, se agregan nuevos dispositivos a initasmdisks. Cuando se reinicia el host, los scripts de inicio mantienen los permisos y la propiedad del dispositivo.

El valor predeterminado para oracleasm.support.without.asmlib es FALSE.

Información relacionada

Dispositivos de partición compatibles

Scripts compatibles

Los scripts asmmain.sh y asmquerydisk.sh permiten cambiar el usuario, el grupo y el usuario de la cuadrícula, todos los cuales se utilizan para consultar los discos ASM. Los scripts siempre deben ejecutarse desde la raíz.

El archivo asmmain.sh es el archivo de secuencia de comandos principal llamado desde cualquier operación que agregue o elimine dispositivos. La secuencia de comandos asmmain.sh llama internamente a otra secuencia de comandos, que debe ejecutarse desde la raíz que tiene las credenciales de la cuadrícula de oracle. Esta secuencia de comandos consulta los dispositivos del grupo de discos ASM y, a continuación, agrega esas entradas en el archivo initasmdisk con el permiso y la propiedad de los dispositivos. Puede cambiar los permisos y la propiedad de este archivo en función del entorno y del patrón regex que se utiliza para hacer coincidir sólo con /dev/mapper/*p1.

La secuencia de comandos asmquerydisk.sh se utiliza para consultar la lista de discos, que se utiliza para crear el grupo de discos ASM. Debe asignar valores a ORACLE_BASE, ORACLE_HOME y ORACLE_SID, según la configuración.

Los scripts están ubicados en /opt/NetApp/smo/plugins/examples/noasmlib. Sin embargo, estos scripts deben moverse a /opt/NetApp/smo/plugins/noasmlib antes de iniciar el servidor SnapManager para Oracle en el host.

Limitaciones de uso de scripts para admitir una base de datos ASM sin ASMLib

Debe tener en cuenta ciertas limitaciones al uso de scripts para admitir una base de

datos ASM sin ASMLib.

- Las secuencias de comandos ofrecen una solución alternativa para cualquier versión del kernel, pero sólo si ASMLib no está instalado.
- Los permisos de los scripts deben definirse de forma que los usuarios root, Grid, oracle o equivalentes puedan acceder a los scripts.
- Los scripts no admiten la restauración desde una ubicación secundaria.

Implementar y ejecutar los scripts

Es posible implementar y ejecutar los scripts asmmain.sh y asmquerydisk.sh para admitir bases de datos ASM sin ASMLib.

Estas secuencias de comandos no siguen la sintaxis de los scripts previos o posteriores y se llama al flujo de trabajo cuando los intitasmdiscos están habilitados. Puede cambiar cualquier cosa relacionada con la configuración en los scripts. Se recomienda verificar si todo lo contenido en los scripts funciona según lo esperado realizando una ejecución de secado rápida.

> Estas secuencias de comandos no afectan a su sistema en caso de fallos ni afectarán a su sistema. Estas secuencias de comandos se ejecutan para actualizar los discos relacionados con ASM para que tengan los permisos y la propiedad adecuados, de modo que los discos siempre estarán bajo control de instancia de ASM.

1. Cree los grupos de discos ASM con los discos con particiones.
2. Cree la base de datos Oracle en LOS GRUPOS de DISCOS.
3. Detenga el servidor SnapManager para Oracle.

   > En un entorno RAC, debe realizar este paso en todos los nodos de RAC.

4. Modifique smo.conf para incluir los siguientes parámetros:

   a. oracleasm.support.without.asmlib = true
   b. oracleasm.support.without.asmlib.owpropiedad = true
   c. oracleasm.support.without.asmlib.username = nombre de usuario del entorno de instancia de ASM
   d. oracleasm.support.without.asmlib.groupname = nombre de grupo del entorno de instancia de ASM

   Estas modificaciones establecen los permisos sólo para la ruta absoluta, lo que significa que en lugar del dispositivo de partición, los permisos se establecerán sólo para el dispositivo dm-*.

5. Modifique los scripts de los plugins disponibles en /opt/NetApp/smo/plugins/examples/noasmlib para incluir los ajustes de configuración en los scripts.
6. Copie las secuencias de comandos en /opt/NetApp/smo/plugins/noasmlib antes de iniciar el servidor SnapManager para Oracle en el host.
7. Desplácese hasta el directorio /opt/NetApp/smo y ejecute una ejecución en seco ejecutando el siguiente script: sh plugins/noasmlib/asmmain.sh

   Se crea el archivo etc/initasmdisks, que es el archivo principal que se utiliza.

   Puede confirmar que el archivo etc/initasmdisks contiene todos los dispositivos relacionados con la base de datos ASM configurada, como:

```
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. Inicie el servidor de SnapManager para Oracle.
9. Configure SnapDrive para UNIX añadiendo lo siguiente al archivo snapdrive.conf.disconnect-luns-before-vbsr=on
10. Reinicie el servidor de SnapDrive para UNIX.

En un entorno RAC, es necesario realizar los pasos del 3 al 10 para todos los nodos RAC.

El archivo /etc/initasmdisks creado, debe ejecutarse desde uno de los scripts de inicio o desde un script que se acaba de definir en rc3.d. El archivo /etc/initasmdisks debe ejecutarse siempre antes de que se inicie el servicio oracleha.

Ejemplo

```
# 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
```

En el ejemplo siguiente, sh -x/etc/initasmdisks no estará disponible de forma predeterminada, y debe anexarlo como primera línea de la función `start_stack()` en un script ohasd:

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

Compatibilidad con bases de datos de ASM de Oracle RAC sin ASMLib

Si utiliza bases de datos Oracle RAC, los nodos RAC deben actualizarse con el archivo

initasmdisks cada vez que se realice una operación en el nodo RAC maestro.

Si no se requiere autenticación para iniciar sesión en los nodos RAC desde el nodo maestro, la asmmain.sh realiza una copia segura (SCP) de inimasmdisks en todos los nodos RAC. El archivo initasmdisks del nodo maestro se llamará cada vez que se produzca la restauración, y la secuencia de comandos asmmain.sh se puede actualizar para invocar la misma secuencia de comandos en todos los nodos RAC.

El archivo /etc/initasmdisks creado que debe ejecutarse desde una de las secuencias de comandos de inicio o desde una secuencia de comandos recientemente definida en rc3.d. El archivo /etc/initasmdisks debe ejecutarse siempre antes de que se inicie el servicio oracleha.

Compatibilidad con bases de datos ASM de Oracle 10g sin ASMLib

Si utiliza Oracle 10g, el comando asmcmd no está disponible para enumerar discos. Puede utilizar la consulta sql para obtener la lista de discos.

La secuencia de comandos disk_list.sql se incluye en las secuencias de comandos existentes proporcionadas en el directorio examples para admitir consultas sql. Al ejecutar el script theasmquerydisk.sh, el script disk_list.sql debe ejecutarse manualmente. Las líneas del script de ejemplo se añaden con comentarios en el archivo asmquerydisk.shI. Este archivo se puede colocar en la ubicación /home/grid u otra ubicación que desee.

Secuencias de comandos de ejemplo para admitir bases de datos ASM sin ASMLib

Los scripts de ejemplo están disponibles en el directorio plugins/examples/noasmlib del directorio de instalación de SnapManager para Oracle.

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$asm_disk;
exit
-bash-4.1$
```

Requisitos para usar bases de datos con NFS y SnapManager

Debe conocer los requisitos para usar las bases de datos con sistema de archivos de red (NFS) y SnapManager. Las recomendaciones incluyen ejecutarse como raíz, caché de atributos y enlaces simbólicos.

- Debe ejecutar SnapManager como raíz; SnapManager debe poder acceder a los sistemas de archivos que contienen archivos de datos, archivos de control, registros de recuperación en línea, registros de archivos y el origen de la base de datos.

  Establezca una de las siguientes opciones de exportación NFS para garantizar que root pueda acceder a los sistemas de archivos:

  - raíz=nombre de host
  - rw=nombre de host, anon=0
- Debe deshabilitar el almacenamiento en caché de atributos para todos los volúmenes que contienen archivos de datos de base de datos, archivos de control, registros de recuperación y archivos, así como el inicio de la base de datos.

  Exporte los volúmenes con las opciones noac (para Solaris y AIX) o actimeo=0 (para Linux).

- Debe vincular los archivos de datos de la base de datos del almacenamiento local a NFS para admitir enlaces simbólicos solamente en el nivel de punto de montaje.

Ejemplos de distribuciones de volúmenes de base de datos

Puede consultar ejemplos de diseños de volumen de base de datos para obtener ayuda en la configuración de la base de datos.

Bases de datos de instancia única

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_sid	Sí	Apagado
Archivos de datos temporales	oratemp_sid	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_sid (multiplexado) Oralog02_sid (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Sí	Apagado

Bases de datos de Real Application Clusters (RAC)

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_dbname	Sí	Apagado
Archivos de datos temporales	oratemp_dbname	Sí	Apagado

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Archivos de control	Oracntrl01_dbname (Multiplexado) Oracntrl02_dbname (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Sí	Apagado
Registros de archivo	oraarch_dbname	Sí	Apagado
Archivos de cluster	oracrs_clustername	Sí	Encendido

Instancia única de una base de datos de Automatic Storage Management (ASM)

Tipos de archivo	Nombres de volúmenes	Nombres de LUN	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	nombre_host de orabin	Sí	Encendido
Archivos de datos	oradata_sid	oradata_sidlun	Sí	Apagado
Archivos de datos temporales	oratemp_sid	OraTemp_sidlun	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Oracntrl01_sidlun (Multiplexado) Oracntrl02_sidlun (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Oralog01_dbnamelun (multiplexado) Oralog02_dbnamelun (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Oraarch_sidlun	Sí	Apagado

Bases de datos RAC ASM

Tipos de archivo	Nombres de volúmenes	Nombres de LUN	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	nombre_host de orabin	Sí	Encendido
Archivos de datos	oradata_sid	oradata_sidlun	Sí	Apagado
Archivos de datos temporales	oratemp_sid	OraTemp_sidlun	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Oracntrl01_sidlun (Multiplexado) Oracntrl02_sidlun (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Oralog01_dbnamelun (multiplexado) Oralog02_dbnamelun (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Oraarch_sidlun	Sí	Apagado
Archivos de cluster	oracrs_clustername	oracrs_clusternamelun	Sí	Encendido

Limitaciones al trabajar con SnapManager

Debe conocer las situaciones y las limitaciones que pueden afectar a su entorno.

Limitaciones relacionadas con diseños y plataformas de bases de datos

- SnapManager admite archivos de control en un sistema de archivos o en un grupo de discos ASM y no admite archivos de control en dispositivos RAW.
- SnapManager funciona en un entorno de cluster Microsoft (MSCS), pero no reconoce el estado de la configuración MSCS (activo o pasivo) y no transfiere la administración activa de un repositorio a un servidor en espera en un clúster MSCS.
- En Red Hat Enterprise Linux (RHEL) y Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 y 5.3 El sistema de archivos ext3 no es compatible al poner en marcha Oracle en dispositivos sin formato mediante multivía dinámica (DMP) en un entorno de I/o de red multivía (MPIO).

  Este problema se observa en SnapManager solo cuando se utiliza SnapDrive 4.1 para UNIX o versiones anteriores.

- SnapManager en RHEL no admite particiones de discos mediante la utilidad **parted**.

Esto es un problema con la utilidad RHEL **parted**.

- En una configuración de RAC, cuando se actualiza un nombre de perfil desde el nodo RAC A, el archivo de programación del perfil se actualiza sólo para el nodo RAC A.

  El archivo de programación para el mismo perfil en el nodo B de RAC no se actualiza y contiene la información de programación anterior. Cuando se activa un backup programado en el nodo B, se produce un error en la operación de backup programada, ya que el nodo B contiene el archivo de programación anterior. Sin embargo, la operación de copia de seguridad programada se realiza correctamente desde el nodo A, en el que se cambia el nombre del perfil. Puede reiniciar el servidor SnapManager para recibir el archivo de programación más reciente para el perfil en el nodo B.

- La base de datos del repositorio puede existir en un host al que se puede acceder mediante más de una dirección IP.

  Si para acceder al repositorio se utiliza más de una dirección IP, se crea el archivo de programación para cada una de las direcciones IP. Si se crea la copia de seguridad de la programación para un perfil (por ejemplo, perfil A) bajo una de las direcciones IP (por ejemplo, IP1), se actualizará el archivo de planificación para sólo esa dirección IP. Si se accede al perfil A desde otra dirección IP (por ejemplo, IP2), la copia de seguridad programada no aparece porque el archivo de programación de IP2 no tiene una entrada para la programación que se creó en IP1.

  Puede esperar a que la programación se active desde esa dirección IP y el archivo de programación que se actualizará o puede reiniciar el servidor.

Limitaciones relacionadas con la configuración de SnapManager

- SnapManager se puede configurar para catalogar backups de bases de datos con RMAN.

  Si se utiliza un catálogo de recuperación de RMAN, el catálogo de recuperación debe estar en una base de datos diferente a la base de datos de la que se realiza el backup.

- SnapDrive para UNIX admite más de un tipo de sistema de archivos y administrador de volúmenes en determinadas plataformas.

  El sistema de archivos y el gestor de volúmenes utilizados para los archivos de la base de datos deben especificarse en el archivo de configuración de SnapDrive como el sistema de archivos predeterminado y el gestor de volúmenes.

- SnapManager admite bases de datos en sistemas de almacenamiento de MultiStore con los siguientes requisitos:
  - Debe configurar SnapDrive para establecer contraseñas para los sistemas de almacenamiento MultiStore.
  - SnapDrive no puede crear una copia snapshot de una LUN o un archivo que reside en un qtree de un sistema de almacenamiento de MultiStore si el volumen subyacente no está en el mismo sistema de almacenamiento de MultiStore.
- SnapManager no admite el acceso a dos servidores SnapManager que se ejecutan en puertos diferentes desde un único cliente (tanto desde la CLI como desde la GUI).

  Los números de puerto deben ser los mismos en los hosts remotos y destino.

- Todas las LUN de un volumen deben estar a nivel de volumen o dentro de qtrees, pero no ambos.

Esto se debe a que, si los datos residen en los qtrees y se monta el volumen, los datos que hay dentro de los qtrees no están protegidos.

- Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

  Es necesario verificar que la base de datos del repositorio esté en ejecución cuando se realiza cualquier operación de SnapManager.

- SnapManager no es compatible con la movilidad de particiones activas (LPM) ni con la movilidad de aplicaciones activas (LAM).
- SnapManager no es compatible con Oracle Wallet Manager ni con el cifrado de datos transparente (TDE).
- SnapManager no admite configuraciones MetroCluster en entornos de asignación de dispositivos sin formato (RDM), ya que las configuraciones de MetroCluster aún deben ser compatibles con Virtual Storage Console (VSC).

Limitaciones relacionadas con la gestión de perfiles

- Si actualiza el perfil para separar los backups de los registros de archivos, no se puede realizar una operación de reversión en el host.
- Si activa un perfil desde la GUI para crear copias de seguridad de registros de archivo y después intenta actualizar el perfil mediante la ventana actualización de perfiles múltiples o la ventana actualización de perfiles, no puede modificar dicho perfil para crear una copia de seguridad completa.
- Si actualiza varios perfiles en la ventana actualización de varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** se desactiva.
- Si actualiza varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** de la ventana actualización de perfiles múltiples está desactivada.
- Si cambia el nombre del perfil, no puede revertir el host.

Limitaciones relacionadas con las operaciones de actualización o reversión

- Si intenta instalar una versión anterior de SnapManager para un host sin realizar la operación de reversión en el host en el repositorio, es posible que no pueda realizar lo siguiente:
  - Ver los perfiles que se crearon en versiones anteriores o posteriores de SnapManager para el host.
  - Acceda a los backups o clones que se crearon en las versiones anteriores o posteriores de SnapManager.
  - Realice operaciones de reversión o actualización en el host.
- Después de separar los perfiles para crear backups de registro de archivos, no se puede ejecutar una operación de reversión en el repositorio de host relacionado.

Limitaciones relacionadas con las operaciones de copia de seguridad

- Se puede producir un error en la creación de backups si se ejecutan operaciones de SnapManager simultáneamente en el mismo host en una base de datos de ASM diferente.
- Durante la recuperación, si el backup ya está montado, SnapManager no volverá a montar el backup y utiliza el backup ya montado.

  Si el backup está montado por un usuario diferente y no tiene acceso al backup montado anteriormente, el

otro usuario debe proporcionarle el permiso.

Todos los archivos de registro de archivos tienen permiso de lectura para los usuarios asignados a un grupo; es posible que no tenga el permiso de acceso al archivo de registro de archivos, si el backup se monta por un grupo de usuarios diferente. Los usuarios pueden otorgar permiso a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la operación de restauración o recuperación.

- SnapManager establece el estado de backup como «PROTEGIDO», incluso cuando una de las copias Snapshot del backup de la base de datos se transfiere al sistema de almacenamiento secundario.
- Puede utilizar el archivo de especificación de tareas para la copia de seguridad programada sólo desde SnapManager 3.2 o posterior.
- Cuando se ejecuta una operación de backup o clonado simultáneamente en las bases de datos de RAC 10gR2 y 11gR2 en ASM, se produce un error en una de las operaciones de creación de clonado o backup.

  Este error se debe a una limitación conocida de Oracle.

- La integración de SnapManager con Protection Manager permite realizar el backup de varios volúmenes en el almacenamiento principal a un único volumen en el almacenamiento secundario para SnapVault y SnapMirror para qtrees.

  No se admite el ajuste de tamaño dinámico de volúmenes secundarios. En la Guía de administración de Provisioning Manager y Protection Manager para usar con DataFabric Manager Server 3.8 encontrará más información al respecto.

- SnapManager no admite copias vault de backups con el script de posprocesamiento.
- Si la base de datos del repositorio apunta a más de una dirección IP y cada dirección IP tiene un nombre de host diferente, la operación de programación de backup se realiza correctamente para una dirección IP, pero falla para la otra dirección IP.
- Después de actualizar a SnapManager 3.4 o una versión posterior, no se podrán actualizar los backups programados con scripts de posprocesamiento que utilicen SnapManager 3.3.1.

  Debe eliminar la programación existente y crear una nueva.

Limitaciones relacionadas con las operaciones de restauración

- Cuando se utiliza un método indirecto para realizar una operación de restauración y los archivos de registro de archivos necesarios para la recuperación solo están disponibles en backups desde el sistema de almacenamiento secundario, SnapManager no logra recuperar la base de datos.

  Esto se debe a que SnapManager no puede montar el backup de los archivos de registro de archivos desde el sistema de almacenamiento secundario.

- Cuando SnapManager realiza una operación de restauración de volúmenes, no se purgan las copias de backup de registros de archivos que se realizan una vez restaurado el backup correspondiente.

  Cuando en el mismo volumen existen los archivos de datos y el destino del archivo de registro de archivos, es posible restaurar los archivos de datos mediante una operación de restauración de volumen si no hay archivos de registro de archivos disponibles en el destino del archivo de registro de archivos. En este caso, se pierden las copias snapshot del registro de archivos que se crean después de la copia de seguridad de los archivos de datos.

  No debe eliminar todos los archivos de registro de archivos del destino del registro de archivos.

- En un entorno ASM, si los archivos de registro de clúster de Oracle (OCR) y de disco de votación coexisten en un grupo de discos que tiene archivos de datos, la operación de vista previa de restauración rápida muestra la estructura de directorio incorrecta para el disco de OCR y de votación.

Limitaciones relacionadas con las operaciones de clonación

- No se puede ver ningún valor numérico entre 0 y 100 en cuanto al progreso de la operación de división de clones debido a la velocidad con la que se detectan y procesan los inodos el sistema de almacenamiento que contiene el volumen flexible.
- SnapManager no admite recibir correos electrónicos solo para las operaciones de división de clones correctamente.
- SnapManager solo admite la división de un FlexClone.
- Se produce un error en la clonado del backup de la base de datos en línea de la base de datos RAC donde se usa la ubicación del archivo de registro de archivos externo debido a un error en la recuperación.

  Se produce un error en la clonado porque Oracle no encuentra y aplica los archivos de registro de archivos para la recuperación desde la ubicación del registro de archivos externo. Esta es una limitación de Oracle. Para obtener más información, consulte el ID de error de Oracle: 13528007. Oracle no aplica el registro de archivo desde la ubicación no predeterminada en la "Sitio de soporte de Oracle". Debe tener un nombre de usuario y una contraseña de Oracle metalink válidos.

- SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.
- Si los espacios de tablas temporales se encuentran en una ubicación diferente a la ubicación de los archivos de datos, una operación de clonado crea los espacios de tabla en la ubicación de los archivos de datos.

  Sin embargo, si los espacios de tablas temporales son Oracle Managed Files (OMF) ubicados en una ubicación diferente a la ubicación de los archivos de datos, la operación de clonado no crea los espacios de tablas en la ubicación de los archivos de datos. SnapManager no gestiona los OMF.

- SnapManager no puede clonar una base de datos de RAC si selecciona la opción -resetlogs.

Limitaciones relacionadas con archivos de registro de archivos y copias de seguridad

- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino de área de recuperación flash.
- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino en espera.
- Los backups de registros de archivos se retienen en función de la duración de la retención y la clase de retención por horas predeterminada.

  Cuando la clase de retención de backup de registros de archivos se modifica mediante la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager, la clase de retención modificada no se considera para el backup porque los backups de registros de archivo se retienen en función de la duración de la retención.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, el backup de registros de archivos no incluye los archivos de registro de archivos más antiguos que el archivo de registro de archivos faltante.

  Si falta el archivo de registro de archivos más reciente, la operación de backup del registro de archivos falla.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.
- SnapManager consolida los backups de registros de archivos incluso cuando se eliminan los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados.

Limitaciones relacionadas con el cambio del nombre de host de la base de datos de destino

No se admiten las siguientes operaciones de SnapManager cuando se cambia el nombre de host de la base de datos de destino:

- Cambiar el nombre de host de la base de datos de destino desde la interfaz gráfica de usuario de SnapManager.
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil.
- Al mismo tiempo, se actualizan varios perfiles para un nuevo nombre de host de base de datos de destino.
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager.

Limitaciones relacionadas con la CLI o GUI de SnapManager

- Los comandos de la CLI de SnapManager para la operación de creación de perfiles que se generan desde la interfaz gráfica de usuario de SnapManager no tienen opciones de configuración del historial.

  No se puede utilizar el comando profile create para configurar las opciones de retención del historial desde la interfaz de línea de comandos de SnapManager.

- SnapManager no muestra la GUI en Mozilla Firefox cuando no hay Java Runtime Environment (JRE) disponible en el cliente UNIX.
- Al actualizar el nombre de host de la base de datos de destino mediante la interfaz de línea de comandos de SnapManager, si hay una o más sesiones abiertas de la interfaz gráfica de usuario de SnapManager, todas las sesiones abiertas de la interfaz gráfica de usuario de SnapManager no pueden responder.

Limitaciones relacionadas con SnapMirror y SnapVault

- El script de posprocesamiento de SnapVault no es compatible si se utiliza Data ONTAP en 7-Mode.
- Si utiliza ONTAP, no puede ejecutar SnapRestore (VBSR) basada en volúmenes en los backups creados en los volúmenes que tienen relaciones de SnapMirror establecidas.

  Esto se debe a una limitación de ONTAP, que no permite romper la relación al realizar una VBSR. Sin embargo, se puede ejecutar un VBSR en el backup último o más reciente creado solo cuando los volúmenes tienen relaciones de SnapVault establecidas.

- Si utiliza Data ONTAP operando en 7-Mode y desea ejecutar un VBSR en los backups creados en los volúmenes que tienen relaciones de SnapMirror establecidas, puede establecer la opción override-vbsr-snapmirror-check en ON en SnapDrive para UNIX.

  La documentación de SnapDrive contiene más información al respecto.

- En algunos casos, no se puede eliminar el último backup asociado con la primera copia Snapshot cuando se ha establecido una relación de SnapVault en el volumen.

  Puede eliminar el backup solo cuando se rompa la relación. Este problema se debe a una restricción de la

ONTAP con copias Snapshot base. En una relación de SnapMirror, la copia de Snapshot básica se crea mediante el motor de SnapMirror y, en una relación de SnapVault, la copia de Snapshot base es el backup creado mediante SnapManager. Para cada actualización, la copia snapshot básica señala el backup más reciente creado mediante SnapManager.

Limitaciones relacionadas con las bases de datos en espera de Data Guard

- SnapManager no admite bases de datos lógicas en espera de Data Guard.
- SnapManager no admite bases de datos en espera de Active Data Guard.
- SnapManager no permite realizar backups en línea de bases de datos Data Guard en espera.
- SnapManager no permite backups parciales de bases de datos en espera de Data Guard.
- SnapManager no permite la restauración de bases de datos Data Guard en espera.
- SnapManager no permite eliminar archivos de registro de archivos para bases de datos en espera de Data Guard.
- SnapManager no admite Data Guard Broker.

Información relacionada

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Limitaciones de SnapManager para Clustered Data ONTAP

Debe conocer las limitaciones de algunas funcionalidades y operaciones de SnapManager si utiliza Clustered Data ONTAP.

Las siguientes funcionalidades no son compatibles si utiliza SnapManager en Clustered Data ONTAP:

- Funcionalidades de protección de datos si SnapManager se integra con Unified Manager de OnCommand
- Una base de datos en la que una LUN pertenece a un sistema que ejecuta Data ONTAP en 7-Mode y la otra LUN pertenece a un sistema que ejecuta Clustered Data ONTAP
- SnapManager para Oracle no admite la migración de un Vserver, que no es compatible con Clustered Data ONTAP
- SnapManager para Oracle no admite la funcionalidad Clustered Data ONTAP 8.2.1 para especificar diferentes políticas de exportación para volúmenes y qtrees

Limitaciones relacionadas con Oracle Database

Antes de empezar a trabajar con SnapManager, debe conocer las limitaciones relacionadas con la base de datos de Oracle.

Estas limitaciones son las siguientes:

- SnapManager es compatible con las versiones 10gR2, 11gR1, 11gR2 y 12*c*_, pero no es compatible con Oracle 10gR1 como repositorio o base de datos de destino.
- SnapManager no admite el uso de una dirección IP DE EXPLORACIÓN en lugar de un nombre de host.

  SCAN IP es una nueva función de Oracle 11gR2.

- SnapManager no es compatible con Oracle Cluster File System (OCFS).
- Oracle 11g en un entorno de NFS directo (dNFS) permite configuraciones de punto de montaje adicionales en el archivo Naranfstab, como varias rutas para el equilibrio de carga.

  SnapManager no modifica el archivo anorfstab. Debe agregar manualmente todas las propiedades adicionales que desee que utilice la base de datos clonada en el archivo oranfstab.

- La compatibilidad con bases de datos Oracle 9i se usa en SnapManager 3.2.
- La compatibilidad con la base de datos Oracle 10gR2 (anterior a 10.2.0.5) queda obsoleta en SnapManager 3.3.1.

> Identifique las distintas versiones de las bases de datos de Oracle que se admiten en la matriz de interoperabilidad.

Información relacionada

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Versiones obsoletas de la base de datos Oracle

SnapManager 3.2 o posterior no admite la base de datos Oracle 9i, y la base de datos Oracle 10gR2 (anterior a 10.2.0.4) no es compatible con SnapManager 3.3.1 o posterior.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o posterior, no puede crear perfiles nuevos; se muestra un mensaje de advertencia.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o una versión posterior, debe realizar una de las siguientes acciones:

- Actualice las bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) a bases de datos de Oracle 10gR2 (10.2.0.5), 11gR1 o 11gR2 y, a continuación, actualice a SnapManager 3.2 o 3.3.

  Si va a actualizar a Oracle 12*c*, debe actualizar a SnapManager 3.3.1 o posterior.

  > La base de datos Oracle 12*c* sólo se admite desde SnapManager 3.3.1.

- Gestión de las bases de datos Oracle 9i mediante una versión de revisión de SnapManager 3.1.

  Puede utilizar SnapManager 3.2 o 3.3 si desea gestionar bases de datos Oracle 10gR2, 11gR1 o 11gR2 y utilizar SnapManager 3.3.1 o posterior si desea gestionar bases de datos Oracle 12*c* junto con otras bases de datos compatibles.

Restricciones en la gestión de volúmenes

SnapManager tiene ciertas restricciones de gestión de volúmenes que pueden afectar al entorno.

Es posible tener varios grupos de discos para una base de datos; sin embargo, las siguientes limitaciones se aplican a todos los grupos de discos de una base de datos determinada:

- Los grupos de discos de la base de datos solo pueden gestionarse un gestor de volúmenes.

- Los dispositivos sin formato respaldados por un gestor de volúmenes lógicos no son compatibles con la protección de los datos de Oracle.

  El almacenamiento de dispositivos sin procesar y los grupos de discos de gestión automática de almacenamiento (ASM) se deben aprovisionar directamente en los dispositivos físicos. En algunos casos, se requiere la partición.

- Un entorno Linux sin gestión de volúmenes lógicos requiere una partición.

Actualizar SnapManager

Puede realizar una actualización a la versión más reciente de SnapManager para Oracle desde cualquiera de las versiones anteriores. Es posible actualizar todos los hosts SnapManager a la vez o realizar una actualización gradual, lo que permite actualizar los hosts de forma escalonada de host por host.

Preparando la actualización de SnapManager

El entorno en el que desea actualizar SnapManager debe cumplir con los requisitos específicos de software, hardware, explorador, base de datos y sistema operativo. Para obtener la información más reciente sobre los requisitos, consulte la matriz de interoperabilidad.

Antes de la actualización, debe asegurarse de realizar las siguientes tareas:

- Complete las tareas de preinstalación necesarias.
- Descargue el último paquete de instalación de SnapManager para Oracle.
- Instalar y configurar la versión adecuada de SnapDrive para UNIX en todos los hosts de destino.
- Crear un backup de la base de datos del repositorio de SnapManager para Oracle existente.

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Actualizar los hosts SnapManager

Es posible actualizar todos los hosts existentes para utilizar la versión más reciente de SnapManager. Todos los hosts se actualizan de forma simultánea. Sin embargo, esto puede provocar un tiempo de inactividad de todos los hosts SnapManager y las operaciones programadas durante ese tiempo.

1. Inicie sesión en el sistema host como usuario raíz.
2. Desde la interfaz de línea de comandos (CLI), desplácese hasta la ubicación donde ha descargado el archivo de instalación.
3. Si el archivo no es ejecutable, cambie los permisos: `chmod 544 netapp.smo*`
4. Detenga el servidor SnapManager: `smo_server stop`
5. En función del host UNIX, instale SnapManager:

Si el sistema operativo es…	A continuación, ejecute…
Solaris (SPARC64)	
Solaris (x86_64)	
AIX (PPC64)	
Linux x86	
Linux x64	

6. En la página Introducción, pulse **Intro** para continuar.

   Aparece el siguiente mensaje: SnapManager existente para Oracle detectado.

7. Pulse **Intro**.
8. En el símbolo del sistema, realice lo siguiente:

   a. Pulse **Intro** para aceptar el valor predeterminado del usuario del sistema operativo.
   b. Introduzca el valor correcto para el grupo de sistemas operativos o pulse **Intro** para aceptar el valor predeterminado.
   c. Introduzca el valor correcto para el tipo de inicio del servidor o pulse **Intro** para aceptar el valor predeterminado.

   Se muestra el resumen de la configuración.

9. Pulse **Intro** para continuar.

   Aparece el siguiente mensaje: Se ha iniciado la desinstalación de SnapManager existente para Oracle.

   La desinstalación ha finalizado y la versión más reciente de SnapManager se ha instalado.

Tareas posteriores a la actualización

Después de actualizar a una versión posterior de SnapManager, es necesario actualizar el repositorio existente. También es posible que desee modificar la clase de retención de backup asignada a la copia de seguridad existente e identificar qué proceso de restauración se puede utilizar.

> Después de actualizar a SnapManager 3.3 o posterior, debe establecer sqlnet.authentication_services a NONE si desea utilizar la autenticación de base de datos (DB) como el único método de autenticación. Esta función no es compatible con las bases de datos RAC.

Actualizando el repositorio existente

No es necesario actualizar el repositorio existente si va a actualizar de SnapManager 3.3.x a SnapManager 3.4 o posterior pero para el resto de las rutas de actualización

debe actualizar el repositorio existente para poder acceder a él después de la actualización.

- El servidor SnapManager actualizado debe haberse iniciado y verificado.
- Debe existir un backup del repositorio existente.
- Si va a actualizar desde cualquier versión anterior a SnapManager 3.1 a SnapManager 3.3 o posterior, primero debe actualizar a SnapManager 3.2.

  Después de actualizar a SnapManager 3.2, puede actualizar a SnapManager 3.3 o una versión posterior.

- Después de actualizar el repositorio, no se puede utilizar el repositorio con una versión anterior de SnapManager.

  a. Actualice el repositorio existente: `smo repository update -repository -dbname repository_service_name -host repository_host_name -login -username repository_user_name -port repository_port`

     - El nombre de usuario del repositorio, el nombre de servicio del repositorio y el nombre de host del repositorio pueden consistir en caracteres alfanuméricos, un signo menos, un guión bajo y un punto.
     - El puerto del repositorio puede ser cualquier número de puerto válido. Las demás opciones utilizadas durante la actualización del repositorio existente son las siguientes:
     - La opción de fuerza
     - La opción noprompt
     - La opción silenciosa
     - La opción verbose

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521

+
```

Reinicie el servidor SnapManager para reiniciar todas las programaciones asociadas.

Modificación de la clase de retención de backups

Después de la actualización, SnapManager asigna la clase de retención de backup predeterminada a los backups existentes. Puede modificar los valores predeterminados de la clase de retención para cumplir sus requisitos de copia de seguridad.

La clase de retención de copias de seguridad predeterminada asignada a las copias de seguridad existentes es la siguiente:

Tipo de backup	Asignación de clase de retención después de la actualización
Los backups se retienen siempre	Ilimitada

Tipo de backup	Asignación de clase de retención después de la actualización
Otros backups	Todos los días

Nota: puede eliminar las copias de seguridad que se conservan para siempre sin cambiar la clase de retención.

Si actualiza a SnapManager 3.0 o posterior, el valor mayor de los siguientes dos valores se asignará a los perfiles existentes:

- Recuento de retención anterior para el perfil
- Valores predeterminados para el recuento de retención y la duración de los backups diarios, como se especifica en el archivo smo.config
  a. Modifique los valores asignados a retain.Hourly.count y Retain.Hourly.Duration en el archivo smo.config.

     Puede introducir los siguientes valores:

     - retain.hourly.count = 12
     - retain.hourly.duration = 2

Información relacionada

Parámetros de configuración de SnapManager

Restaurar tipos de proceso

Todas las versiones de SnapManager para Oracle no admiten todos los procesos de restauración. Después de actualizar SnapManager, debe tener en cuenta el proceso de restauración que puede usar para restaurar un backup.

Los backups creados con SnapManager 3.0 o versiones posteriores pueden restaurarse utilizando procesos rápidos de restauración y restauración basada en archivos. Sin embargo, los backups creados con una versión anterior a SnapManager 3.0 se pueden restaurar utilizando únicamente el proceso de restauración basada en archivos.

Puede determinar la versión de SnapManager utilizada para crear el backup mediante la ejecución del comando -backup show.

Información relacionada

Qué es la restauración de base de datos

Actualizar hosts de SnapManager mediante actualización gradual

El enfoque de actualización gradual que permite actualizar los hosts de forma escalonada y host por host se admite desde SnapManager 3.1.

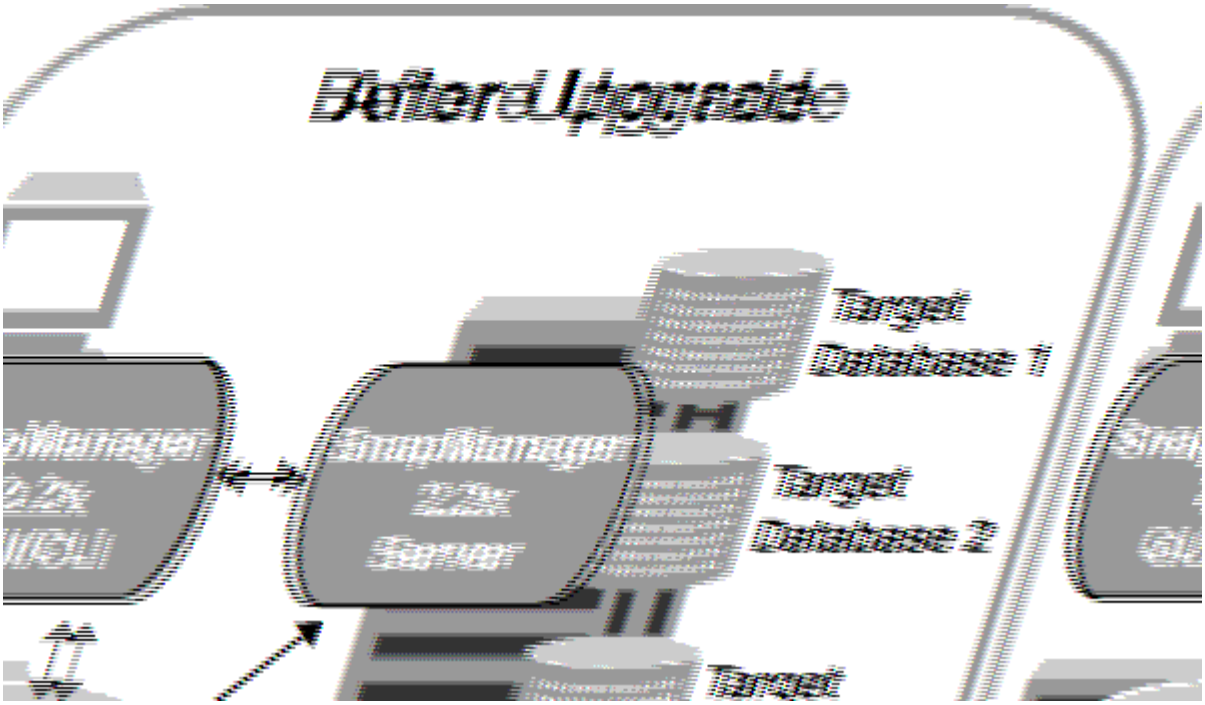
SnapManager 3.0 o versiones anteriores solo permitió actualizar todos los hosts al mismo tiempo. Esto provocó un tiempo de inactividad de todos los hosts SnapManager y las operaciones programadas durante la

operación de actualización.

La actualización gradual ofrece las siguientes ventajas:

- Se ha mejorado el rendimiento de SnapManager porque solo se actualiza un host a la vez.
- Capacidad para probar las nuevas funciones en un host de servidor SnapManager antes de actualizar los otros hosts.

> Solo se puede realizar la actualización gradual mediante la interfaz de línea de comandos (CLI).



Después de completar correctamente la actualización, los hosts de SnapManager, los perfiles, las programaciones, las backups, Además, los clones asociados con los perfiles de las bases de datos de destino se migran de la base de datos del repositorio de la versión de SnapManager anterior a la base de datos del repositorio de la nueva versión. Los detalles sobre las operaciones realizadas mediante los perfiles, las programaciones, los backups y los clones que se crearon con la versión anterior de SnapManager ahora están disponibles en la base de datos del repositorio de la nueva versión. Puede iniciar la GUI utilizando los valores de configuración predeterminados del archivo user.config. No se consideran los valores configurados en el archivo user.config de la versión anterior de SnapManager.

El servidor SnapManager actualizado ahora puede comunicarse con la base de datos del repositorio actualizada. Los hosts que no se actualizaron pueden gestionar sus bases de datos de destino mediante el repositorio de la versión anterior de SnapManager y, por lo tanto, pueden utilizar las funciones disponibles en la versión anterior.

> Antes de realizar la actualización gradual, debe asegurarse de que todos los hosts de la base de datos del repositorio puedan resolverse. Para obtener información acerca de cómo resolver los hosts, consulte la sección de solución de problemas en *SnapManager for Oracle Administration Guide for UNIX*.

Información relacionada

Qué es una reversión

Requisitos previos para realizar actualizaciones sucesivas

Antes de realizar una actualización gradual, debe asegurarse de que el entorno cumpla con ciertos requisitos.

- Si utiliza cualquier versión anterior a SnapManager 3.1 y desea realizar una actualización gradual a SnapManager 3.3 o posterior, primero debe actualizar a la versión 3.2 y, después, a la última.

  Puede actualizar directamente de SnapManager 3.2 a SnapManager 3.3 o posterior.

- Deben realizarse backups de los scripts externos que se usan para realizar cualquier protección de datos externa o retención de datos.
- Debe instalarse la versión de SnapManager a la que desea actualizar.

  Si va a actualizar desde cualquier versión anterior a SnapManager 3.1 a SnapManager 3.3 o posterior, primero debe instalar SnapManager 3.2 y realizar una actualización gradual. Después de actualizar a la versión 3.2, puede instalar SnapManager 3.3 o posterior y realizar otra actualización gradual a SnapManager 3.3 o posterior.

- Debe instalarse la versión de SnapDrive para UNIX compatible con la versión de SnapManager a la que desea actualizar.

  La documentación de SnapDrive contiene detalles sobre la instalación de SnapDrive.

- Debe realizarse un backup de la base de datos del repositorio.
- La cantidad de utilización de repositorio de SnapManager debe ser mínima.
- Si el host que se va a actualizar utiliza un repositorio, no deben realizarse operaciones de SnapManager en los demás hosts que utilizan el mismo repositorio.

  Las operaciones que están programadas o en ejecución en los otros hosts esperan a que finalice la actualización gradual.

  Se recomienda realizar una actualización gradual cuando el repositorio esté menos ocupado, como durante el fin de semana o cuando las operaciones no estén programadas.

- Los perfiles que apuntan a la misma base de datos de repositorio deben crearse con nombres diferentes en los hosts de servidor SnapManager.

  Si utiliza perfiles con el mismo nombre, la actualización gradual que implica esa base de datos del repositorio falla sin previo aviso.

- No deben realizarse operaciones de SnapManager en el host que se está actualizando.

  La actualización gradual se ejecuta durante más tiempo a medida que aumenta el número de backups de los hosts que se van actualizando conjuntamente. La duración de la actualización puede variar según la cantidad de perfiles y backups asociados con un host determinado.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Realizar la actualización gradual en un único host o en varios hosts

Puede realizar la actualización gradual en un único o varios hosts de servidor SnapManager mediante la interfaz de línea de comandos (CLI). El host del servidor SnapManager actualizado se gestiona únicamente con la versión posterior de SnapManager.

Debe asegurarse de que se hayan completado todos los requisitos previos para realizar la actualización gradual.

1. Para realizar una actualización sucesiva en un solo host, introduzca el siguiente comando: 'Morepipository rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-upgrade-hosthost_with_target_database-force [-quiet | -verbose]'

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino montadas en Hosta y una base de datos de repositorio denominada REPOA ubicada en repo_host:

   ```
   smo repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA
   ```

2. Para realizar una actualización sucesiva en varios hosts, introduzca el siguiente comando: 'Morepostory rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-upgrade-hoshost_with_target_database1,host_with_target_target_enset_encally] [-verbose]

   > Para varios hosts, introduzca los nombres de hosts separados por una coma y asegúrese de no incluir espacio entre la coma y el siguiente nombre de host.Si utiliza una configuración RAC, debe actualizar manualmente todos los hosts asociados con RAC. Puede utilizar -allhosts para realizar la actualización gradual de todos los hosts.

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino montadas en los hosts, Hosta y HostB y una base de datos de repositorio denominada REPOA ubicada en repo_host:

   ```
   smo repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA,hostB
   ```

3. Para realizar una actualización sucesiva en todos los hosts de una base de datos de repositorio, introduzca el siguiente comando: 'Morepisitory rollingupgrade-repository-dbnamerepo_service_name-strepo_host-login-usernamerepo_username-portrepo_Port-allhosts-force [-quiet | -verbose]'

   Después de actualizar correctamente la base de datos de repositorio, puede realizar todas las operaciones de SnapManager en la base de datos de destino.

   La actualización de SnapManager para Oracle conserva las credenciales de usuario basadas en host, las credenciales de usuario del software de Oracle y las credenciales de usuario de Oracle Recovery Manager (RMAN) desde la versión anterior de SnapManager para Oracle.

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino disponibles en una base de datos de repositorio denominada REPOA ubicada en repo_host:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
      -allhosts
```

   - Si el servidor SnapManager se inicia automáticamente, debe reiniciar el servidor para garantizar que pueda ver las programaciones.
   - Si actualiza uno de los dos hosts relacionados, debe actualizar el segundo host después de actualizar el primero.

     Por ejemplo, si ha creado un clon del host A al host B o montado un backup del host A al host B, los hosts A y B están relacionados entre sí. Cuando se actualiza el host A, aparece un mensaje de advertencia en el que se le solicita actualizar el host B poco después de actualizar el host A.

     > Los mensajes de advertencia se muestran aunque el clon se elimina o el backup se desasocia del host B durante la actualización gradual del host A. Esto se debe a que existen metadatos en el repositorio para las operaciones realizadas en el host remoto.

Información relacionada

Requisitos previos para realizar actualizaciones sucesivas

Qué es una reversión

La operación de reversión permite revertir a una versión anterior de SnapManager después de realizar una actualización gradual.

> Antes de realizar una reversión, debe asegurarse de que todos los hosts en la base de datos del repositorio puedan resolverse.

Al realizar una reversión, se revierte lo siguiente:

- Los backups creados, liberados y eliminados mediante la versión de SnapManager desde la que se está revirtiendo
- Los clones creados a partir de un backup que se creó mediante la versión de SnapManager a partir de la cual se va a revertir
- Las credenciales de perfil modificadas por medio de la versión de SnapManager de la que se va a revertir
- Estado de protección del backup modificado mediante la versión de SnapManager de la cual se va a revertir

No se admiten las funciones disponibles en la versión de SnapManager que utilizaba, pero no están disponibles en la versión en la que se está revirtiendo. Por ejemplo, cuando realiza una reversión desde SnapManager 3.3 o posterior a SnapManager 3.1, la configuración de historial establecida para perfiles en SnapManager 3.3 o posterior no se revierte a los perfiles en SnapManager 3.1. Esto se debe a que la característica de configuración del historial no estaba disponible en SnapManager 3.1.

Información relacionada

Resolución de problemas de SnapManager

Limitaciones en la ejecución de una reversión

Debe conocer cuáles son las situaciones en las que no se puede ejecutar una reversión. No obstante, en algunas de estas situaciones es posible ejecutar algunas tareas adicionales antes de realizar la reversión.

Los casos en los que no se puede ejecutar la reversión o se debe realizar las tareas adicionales son los siguientes:

- Si realiza una de las siguientes operaciones después de realizar una actualización gradual:
  - Cree un nuevo perfil.
  - Divida un clon.
  - Cambie el estado de protección del perfil.
  - Asigne una política de protección, una clase de retención o las relaciones de SnapVault y SnapMirror.

    En esta situación, después de ejecutar una reversión, debe quitar manualmente la política de protección, la clase de retención o las relaciones SnapVault y SnapMirror asignadas.

  - Cambie el estado de montaje del backup.

    En este caso, primero debe cambiar el estado de montaje a su estado original y, a continuación, ejecutar una reversión.

  - Restaurar un backup.
  - Cambie el modo de autenticación de la autenticación de la base de datos a la autenticación del sistema operativo (SO).

    En esta situación, después de realizar una reversión, debe cambiar manualmente el modo de autenticación de sistema operativo a base de datos.

- Si se cambia el nombre de host del perfil
- Si se separan perfiles para crear backups de registros de archivo

En este caso, no puede volver a una versión anterior a SnapManager 3.2.

Requisitos previos para ejecutar una reversión

Antes de realizar una reversión, debe asegurarse de que el entorno cumpla con ciertos requisitos.

- Si utiliza SnapManager 3.3 o una versión posterior y desea revertir a una versión anterior a SnapManager 3.1, tendrá que volver a la versión 3.2 y, a continuación, a la versión deseada.
- Deben realizarse backups de los scripts externos que se usan para realizar cualquier protección de datos externa o retención de datos.
- Debe instalarse la versión de SnapManager a la que desea revertir.

> Si desea realizar una reversión de SnapManager 3.3 o posterior a una versión anterior a SnapManager 3.1, primero debe instalar SnapManager 3.2 y realizar una reversión. Después de revertir a 3.2, puede instalar SnapManager 3.1 o una versión anterior y realizar otra reversión a esa versión.

- Debe instalarse la versión de SnapDrive para UNIX compatible con la versión de SnapManager a la que desea revertir.

  Para obtener información sobre la instalación de SnapDrive, consulte el conjunto de documentación de SnapDrive.

- Debe realizarse un backup de la base de datos del repositorio.
- Si el host que se va a revertir utiliza un repositorio, no debe realizarse operaciones de SnapManager en los demás hosts que utilizan el mismo repositorio.

  Las operaciones que están programadas o en ejecución en los otros hosts esperan a que se complete la reversión.

- Los perfiles que apuntan a la misma base de datos del repositorio deben crearse con nombres diferentes en los hosts del servidor SnapManager.

  Si se utilizan perfiles con el mismo nombre, la operación de reversión que implica la base de datos del repositorio generará un error sin previo aviso.

- No se deben realizar operaciones de SnapManager en el host al que se desea revertir.

  Si existe una operación en ejecución, debe esperar hasta que se complete esa operación y antes de continuar con la reversión.

> La operación de reversión se ejecuta durante más tiempo a medida que aumenta la cantidad acumulativa de backups de los hosts que se están revertir juntos. La duración de la reversión puede variar según la cantidad de perfiles y backups asociados con un host determinado.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Ejecución de una reversión en un solo host o varios hosts

Puede realizar una reversión en una sola o varios hosts de servidor SnapManager con la

interfaz de línea de comandos (CLI).

Se debe asegurarse de que se hayan completado todos los requisitos previos para realizar una reversión.

1. Para realizar una reversión en un solo host, introduzca el siguiente comando: `smorepository rollback-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_port-rollbackhosthost_with_target_database`

   En el ejemplo siguiente se muestra el comando para revertir todas las bases de datos de destino montadas en Hosta y una base de datos de repositorio denominada REPOA ubicada en el host de repositorio, repo_host:

   ```
   smo repository rollback
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -rollbackhost hostA
   ```

2. Para realizar una reversión en varios hosts, introduzca el siguiente comando: Smorepostory rollback-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-rollbackhoshost_with_target_database1,host_with_target_target_database2

   > Si desea introducir varios hosts, introduzca los nombres de host separados por una coma y asegúrese de que no haya espacio entre la coma y el siguiente nombre de host.

   Si utiliza una configuración de RAC, debe revertir manualmente todos los hosts asociados de RAC. Es posible utilizar -allhosts para realizar una reversión de todos los hosts.

   En el ejemplo siguiente se muestra el comando para revertir todas las bases de datos de destino montadas en los hosts, Hosta, HostB y una base de datos de repositorio denominada REPOA ubicada en el host de repositorios, repo_host:

   ```
   smo repository rollback
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -rollbackhost hostA,hostB
   ```

   Los hosts, los perfiles, las programaciones, los backups y los clones que están asociados con los perfiles de las bases de datos de destino para el host se revierten al repositorio anterior.

Información relacionada

Tareas posteriores a la reversión

Es necesario realizar algunos pasos adicionales después de revertir una base de datos de repositorio y degradar el host de SnapManager de SnapManager 3.2 a SnapManager 3.0, para ver las programaciones creadas en la versión anterior de la base de datos del repositorio.

1. Desplácese hasta cd /opt/NetApp/smo/repositorios.

   El directorio de repositorios puede contener dos archivos para cada repositorio. El nombre de archivo con el signo de número (#) se crea utilizando SnapManager 3.1 o posterior y el nombre de archivo con el guión (-) se crea utilizando SnapManager 3.0.

   Los nombres de los archivos pueden ser los siguientes:

   - Repository#SMO300a#SMOREPO1#10.72.197.141#1521
   - repository-smo300a-smorepo1-10.72.197.141-1521
2. Reemplace el signo de número (#) en el nombre de archivo por el guión (-).

   El nombre de archivo que tenía el signo de número (#) contiene ahora guión (-): Repository-SMO300a-SMOREPO1-10.72.197.141-1521.

Configurando SnapManager

Después de instalar SnapManager, debe realizar algunas tareas de configuración adicionales según el entorno que utilice.

Parámetros de configuración de SnapManager

SnapManager proporciona una lista de parámetros de configuración que se pueden editar en función de sus requisitos. Los parámetros de configuración se almacenan en el archivo smo.config. Sin embargo, es posible que el archivo smo.config no contenga todos los parámetros de configuración admitidos. Puede agregar los parámetros de configuración, según sus necesidades.

En la siguiente tabla, se enumeran todos los parámetros de configuración de SnapManager compatibles y también se explica cuándo usar estos parámetros:

Parámetros	Descripción

• retain.hourly.count • retain.hourly.duration • retenga.monthly.count • retain.monthly.duration	Estos parámetros configuran la política de retención al crear un perfil. Por ejemplo, puede asignar los siguientes valores:retain.Hourly.count = 12 retain.hourly.duration = 2 retenga.monthly.count = 2 retain.monthly.duration = 6
restore.secondaryAccessPolicy	Este parámetro define cómo SnapManager puede acceder a los datos en el almacenamiento secundario cuando no puede restaurarse directamente con Protection Manager. Las diferentes maneras de acceder a los datos en el almacenamiento secundario son las siguientes: • Directo (predeterminado) Cuando restore.secondaryAccessPolicy está configurado como directa, SnapManager clona los datos en el sistema de almacenamiento secundario, monta los datos clonados del almacenamiento secundario en el host, y, a continuación, copia los datos del clon en el entorno activo. • Indirecto Si asigna de forma indirecta a restore.secondaryAccessPolicy, SnapManager copia datos en un volumen temporal del sistema de almacenamiento principal, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal al entorno activo. El método indirecto se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Este método tarda el doble de tiempo que el método directo porque se realizan dos copias de los datos. En una red de área de almacenamiento (SAN) con sistema de archivos de red (NFS) como protocolo, SnapManager no necesita conectarse directamente al almacenamiento secundario para realizar una restauración.

Restore.temporaryVolumeName	Este parámetro asigna un nombre al volumen temporal. Cuando SnapManager utiliza el método indirecto para restaurar datos desde el almacenamiento secundario, requiere un volumen de desecho en el almacenamiento principal para conservar una copia temporal de los datos hasta que se copian en los archivos de la base de datos y se recupera la base de datos. No hay un valor predeterminado. Si no especifica un valor, debe introducir un nombre en el comando restore que utilice el método indirecto. Por ejemplo, puede asignar los siguientes valores:restore.temporaryVolumeName = smo_temp_volume
Retenga.always Freepiredbackups	Este parámetro permite a SnapManager liberar backups cuando caduquen y cuando se realice una restauración rápida, incluso si no se configuró la protección de datos. Este parámetro libera los backups protegidos que caducan y eliminan los backups sin proteger que caducan. Los posibles valores que puede asignar son los siguientes: • Verdadero Si asigna true a retain.alforms FreeExpiredbackups, SnapManager libera las copias de seguridad caducadas independientemente de si las copias de seguridad están protegidas. Los backups se eliminan cuando no están protegidos o si las copias protegidas en el almacenamiento secundario también han caducado. • Falso Si asigna false a retain.alforms FreeExpiredbackups, SnapManager libera las copias de seguridad caducadas que están protegidas.

host.credenciales.persistir	Este parámetro permite que SnapManager almacene credenciales del host. De manera predeterminada, las credenciales del host no se almacenan. Sin embargo, se deben almacenar las credenciales de host si tiene un script personalizado que se ejecuta en un clon remoto y requiere acceso a un servidor remoto. Para habilitar el almacenamiento de credenciales de host, asigne TRUE al host.credenciales.persistir. SnapManager cifra y guarda las credenciales del host.
RestorePlanMaxFilesDisjugado	Este parámetro permite definir el número máximo de archivos que se mostrarán en la vista previa de la restauración.de forma predeterminada, SnapManager muestra un máximo de 20 archivos en la vista previa de la restauración. Sin embargo, puede cambiar a un valor mayor que 0. Por ejemplo, puede asignar el siguiente valor: • RestorePlanMaxFilesDisjugado = 30 Si especifica un valor no válido, se muestra el número predeterminado de archivos.
snapshot.list.timeout.min	Este parámetro permite definir el tiempo en minutos durante el cual SnapManager debe esperar a que se ejecute el comando snap list al realizar cualquier operación de SnapManager.de forma predeterminada, SnapManager espera 30 minutos. Sin embargo, puede cambiar a un valor mayor que 0. Por ejemplo, puede asignar el siguiente valor: • snapshot.list.timeout.min = 40 Si especifica un valor no válido, se utiliza el valor predeterminado. Para cualquier operación de SnapManager, si el tiempo de ejecución del comando snap list supera el valor asignado a snapshot.list.timeout.min, la operación genera un mensaje de error de tiempo de espera.

PruneIfFileExistsInOtherDestination	Este parámetro de eliminación permite definir el destino de los archivos de registros de archivos. Los archivos de registro de archivos se almacenan en varios destinos. Al eliminar los archivos de registro de archivos, SnapManager debe conocer el destino de los archivos de registro de archivos. Los posibles valores que puede asignar son los siguientes: • Cuando desee quitar los archivos de registro de archivo de un destino especificado, debe asignar false a pruneIfFileExistsInOtherDestination. • Cuando desee quitar los archivos de registro de archivo de un destino externo, debe asignar true a pruneIfFileExistsInOtherDestination.
prune.archivelogs.backedup.from.otherdestination	Este parámetro de eliminación permite reducir los archivos de registro de archivos de los que se ha realizado una copia de seguridad desde los destinos de registro de archivos especificados o del que se ha realizado una copia de seguridad desde destinos de registros de archivos externos. Los posibles valores que puede asignar son los siguientes: • Si desea comprimir los archivos de registro de archivos desde los destinos especificados y si se realiza un backup de los archivos de registro de archivos desde los destinos especificados mediante -prune-dest, debe asignar false a prune.archivelogs.backedup.from.otherdestination . • Si desea comprimir los archivos de registro de archivos desde destinos especificados y si se realiza una copia de seguridad de los archivos de registro de archivos al menos una vez desde cualquiera de los otros destinos, debe asignar true a prune.archivelogs.backedup.from.otherdestination .
Maximum.archivvelog.files.torune.atATime	Este parámetro de eliminación permite definir el número máximo de archivos de registro de archivos que puede recortar en un momento dado. Por ejemplo, puede asignar el siguiente valor:Maximum.archivvelog.files.torune.atATime = 998 El valor que se puede asignar a Maximum.archivvelog.files.torune.atATime debe ser inferior a 1000.

archvelogs.consolidate	Este parámetro permite a SnapManager liberar las copias de seguridad duplicadas de registros de archivo si asigna true a archivvelogs.consolidate.
suffix.backup.label.with.logs	Este parámetro permite especificar el sufijo que se desea añadir para diferenciar los nombres de etiqueta del backup de datos y del backup de registros de archivo.por ejemplo, al asignar registros al sufijo.backup.label.with.logs, se añade _logs como sufijo a la etiqueta de backup de registros de archivo. La etiqueta de backup del registro de archivos debería ser arch_logs.
backup.archivelogs.beyond.missingfiles	Este parámetro permite que SnapManager incluya los archivos de registro de archivos faltantes en el backup. Los archivos de registro de archivos que no existen en el sistema de archivos activo no se incluyen en la copia de seguridad. Si desea incluir todos los archivos de registro de archivos, incluso los que no existen en el sistema de archivos activo, debe asignar true a backup.archivelogs.beyond.missingfiles. Puede asignar false para ignorar los archivos de registro de archivos que faltan.
srvctl.timeout	Este parámetro permite definir el valor de tiempo de espera para el comando srvctl. **Nota:** el control de servidor (SRVCTL) es una utilidad para administrar instancias de RAC. Cuando SnapManager tarda más tiempo en ejecutar el comando srvctl que el valor timeout, la operación SnapManager produce un error con este mensaje de error: Error: Se ha agotado el tiempo de espera mientras se ejecuta el comando: Srvctl status.
Snapshot.restore.storageNameCheck	Este parámetro permite a SnapManager ejecutar la operación de restauración con copias de Snapshot que se crearon antes de migrar desde operaciones de Data ONTAP en 7-Mode a Clustered Data ONTAP.el valor predeterminado asignado al parámetro es FALSE. Si ha realizado la migración desde Data ONTAP funcionando en 7-Mode a Clustered Data ONTAP, pero quiere utilizar las copias Snapshot creadas antes de la migración, establezca snapshot.restore.storageNameCheck=true.

services.common.disableAbort	Este parámetro deshabilita la limpieza tras el fallo de las operaciones de ejecución prolongada. Puede establecer un ejemplo services.common.disableAbort=true.For, si está realizando una operación de clonado que se ejecuta mucho y, a continuación, se produce un error debido a un error de Oracle, es posible que no desee limpiar el clon. Si establece services.common.disableAbort=true, no se eliminará el clon. Puede corregir el problema de Oracle y reiniciar la operación de clonado desde el punto en que falló.
• backup.sleep.dnfs.layout • backup.sleep.dnfs.secs	Estos parámetros activan el mecanismo de suspensión en el diseño Direct NFS (dNFS). Después de crear la copia de seguridad de los archivos de control con dNFS o un sistema de archivos de red (NFS), SnapManager intenta leer los archivos de control, pero es posible que no se encuentren los archivos.para habilitar el mecanismo de suspensión, asegúrese de que backup.sleep.dnfs.Layout=true. El valor predeterminado es TRUE. Al activar el mecanismo de suspensión, debe asignar el tiempo de suspensión a backup.sleep.dnfs.secs. El tiempo de inactividad asignado es en segundos y el valor depende de su entorno. El valor predeterminado es 5 segundos. Por ejemplo: • backup.sleep.dnfs.layout=true • backup.sleep.dnfs.secs=2

• override.default.backup.pattern • new.default.backup.pattern	Cuando no se especifica la etiqueta de backup, SnapManager crea una etiqueta de backup predeterminada. Estos parámetros de SnapManager permiten personalizar la etiqueta de copia de seguridad predeterminada.para personalizar la etiqueta de copia de seguridad, asegúrese de que el valor de override.default.backup.pattern se establece en true. El valor predeterminado es FALSE. Para asignar el nuevo patrón de la etiqueta de backup, se pueden asignar palabras clave como el nombre de la base de datos, el nombre del perfil, el ámbito, el modo y el nombre del host a new.default.backup.pattern. Las palabras clave se deben separar con un guión bajo. Por ejemplo, new.default.backup.pattern=dbname_profile_hostname_scope_mode. La Marca de hora se incluye automáticamente al final de la etiqueta generada.
allow.underscore.in.clone.sid	Oracle admite el uso de guion bajo en el SID de clonado de Oracle 11gR2. Este parámetro SnapManager permite incluir un guión bajo en el nombre del SID del clon.para incluir un guión bajo en el nombre del SID del clon, asegúrese de que el valor de allow.underscore.in.clone.sid se configure en TRUE. El valor predeterminado es TRUE. Si utiliza una versión de Oracle anterior a Oracle 11gR2 o si no desea incluir un guión bajo en el nombre del SID del clon, establezca el valor en FALSE.
oracle.parameters.with.comma	Este parámetro permite especificar todos los parámetros de Oracle que tienen coma (,) como valor.mientras se realiza cualquier operación, SnapManager usa oracle.parameters.with.comma para comprobar todos los parámetros de Oracle y omitir la división de los valores. Por ejemplo, si el valor de nls_numeric_characters=, especifique oracle.parameters.with.comma=nls_numeric_characters. Si hay varios parámetros de Oracle con coma como valor, debe especificar todos los parámetros en oracle.parameters.with.comma.

• ArchivedLogs.Exclude • ArchivedLogs.exclude.fileslike • <db-unique-name>.archivedLogs.exclude.fileslike	Estos parámetros permiten a SnapManager excluir los archivos de registro de archivado de los perfiles y las copias de seguridad si la base de datos no está en un sistema de almacenamiento habilitado para la copia snapshot y desea realizar operaciones SnapManager en ese sistema de almacenamiento.**Nota:** debe incluir los parámetros de exclusión en el archivo de configuración antes de crear un perfil. Los valores asignados a estos parámetros pueden ser un directorio de nivel superior o un punto de montaje donde están presentes los archivos de registro de archivos o un subdirectorio. Si se especifica un directorio de nivel superior o un punto de montaje y si la protección de datos está habilitada para un perfil en el host, ese punto o directorio de montaje no se incluye en el conjunto de datos que se crea en Protection Manager. Cuando existen varios archivos de registro de archivos para excluirse del host, debe separar las rutas de los archivos de registro de archivos mediante comas. Para excluir los archivos de registro de archivos de que se incluyan en el perfil y se realice una copia de seguridad, debe incluir uno de los parámetros siguientes: • ArchivedLogs.exclude para especificar una expresión regular para excluir los archivos de registro de archivos de todos los perfiles o copias de seguridad. Los archivos de registro de archivos que coinciden con la expresión regular se excluyen de todos los perfiles y copias de seguridad. Por ejemplo, puede establecer archivedLogs.exclude = /arch/logs/on/local/disk1/.,**/arch/logs/on/local/disk2/.**. Para las bases de datos de ASM, puede establecer archivedLogs.exclude = \\+KHDB_ARCH_DEST/khdb/archivvelog/.,**\\+KHDB_NNAARCHTWO/khdb/archivvelog/.**. • ArchivedLogs.exclude.filesLike de especificar una expresión SQL para excluir los archivos de registro de archivos de todos los perfiles o copias de seguridad. Los archivos de registro de archivos que coinciden con la expresión SQL se excluyen de todos los perfiles y las copias de seguridad. Por ejemplo, puede establecer archivedLogs.exclude.fileslike = /arch/logs/on/local/disk1/%,/arch/logs/on/local/disk2/%.

Edición de los parámetros de configuración

Según el entorno, puede cambiar los valores predeterminados asignados al parámetro de configuración.

1. Abra el archivo de configuración desde la siguiente ubicación predeterminada:

   ubicación/propiedades de la instalación predeterminada/smo.config

2. Cambie los valores predeterminados de los parámetros de configuración.

   > También puede agregar parámetros de configuración compatibles que no se incluyen en el archivo de configuración y asignarles valores.

3. Reinicie el servidor de SnapManager para Oracle.

- <db-unique-name>.ArchivedLogs.exclude.filesLike para especificar una expresión SQL para excluir los archivos de registro de archivos sólo del perfil o la copia de seguridad creada para la base de datos con el nombre único dB especificado.

  Los archivos de registro de archivos que coinciden con la expresión SQL se excluyen del perfil y las copias de seguridad.

  Por ejemplo, puede establecer mydB.archivedLogs.exclude.fileslike = /arch/logs/on/local/disk1/%,/arch/logs/on/local/disk2/%.

Configuración de SnapDrive para UNIX para un entorno activo/activo de Veritas SFRAC

Si ha incluido el parámetro host-cluster-sw-restore-warn en snapdrive.conf y ha asignado el valor on, debe cambiar el valor para admitir la operación de restauración en el entorno activo/activo de Veritas Storage Foundation para Oracle RAC (SFRAC).

Cuando se utiliza el entorno Active/active Veritas Storage Foundation para Oracle RAC (SFRAC), si el parámetro host-cluster-sw-restore-warn está activado, se muestra un mensaje de advertencia y se detiene la operación de restauración. Si desea realizar la operación de restauración en un entorno Veritas SFRAC activo/activo, debe establecer host-cluster-sw-restore-warn en OFF.

Para obtener más información sobre snapdrive.conf, consulte la documentación de SnapDrive.

1. Inicie sesión como usuario root.
2. Abra el archivo snapdrive.conf mediante un editor de texto.
3. Cambie el valor host-cluster-sw-restore-warn a OFF.

Tras la configuración, reinicie el servidor SnapDrive para UNIX.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Configurar SnapManager para que sea compatible con el entorno de Veritas SFRAC

Cuando se instala SnapManager en Solaris, puede configurar SnapManager para que sea compatible con el entorno de Veritas Storage Foundation para Oracle RAC (SFRAC).

- El host debe tener Solaris, utilidades host y Veritas instalados.
  a. Cree un grupo de discos compartidos y un sistema de archivos para SnapManager mediante SnapDrive para UNIX para que los sistemas de archivos se monten simultáneamente en ambos nodos de Real Application Clusters (RAC).

     Para obtener información acerca de cómo crear un grupo de discos compartidos y un sistema de archivos, consulte la documentación de SnapDrive.

b. Instalar y configurar la base de datos Oracle que se va a montar en los sistemas de archivos compartidos.

c. Inicie una instancia de base de datos en cualquier nodo del RAC.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Asegurarse de que ASM detecta discos importados

Si utiliza Automatic Storage Management (ASM) en un entorno NFS, después de instalar SnapManager, debe asegurarse de que ASM pueda detectar los discos importados por SnapManager. Para ello, puede añadir la ruta del directorio ASM al parámetro ASM_DISKSTRING.

Puede utilizar herramientas de Oracle para editar el parámetro ASM_DISKSTRING. Para obtener información acerca de la edición de ASM_DISKSTRING, consulte la documentación de Oracle.

La ruta de acceso del disco ASM /opt/NetApp/smo/mnt//disk*' debe agregarse a la ruta de acceso existente definida en el parámetro ASM_DISKSTRING. Por ejemplo, si la ruta definida en ASM_DISKSTRING era /mnt/my-asm-disks/dir1/disk*, después de agregar la ruta de acceso del disco ASM, la ruta actualizada será '/mnt/my-asm-disks/dir1/disk*,/opt/NetApp/smo/mnt//disk*'.

> El parámetro ASM_DISKSTRING debe coincidir solo con los archivos de disco de ASM y no con ningún otro archivo.

- El primer asterisco (*) indica el nombre generado por SnapManager para el punto de montaje raíz.
- El segundo * indica el directorio dentro del punto de montaje.
- El tercer * indica el nombre del archivo NFS.

Debe asegurarse de que el * coincida con la topología de su sistema de archivos NFS si el disco está montado en los directorios de /opt/NetApp/smo/mnt/<smo-generated-name>/.

1. Si utiliza discos ASM con NFS en el entorno de almacenamiento conectado a la red (NAS), edite el parámetro ASM_DISKSTRING de modo que apunte a la ruta del directorio ASM actual.

   Si el punto de montaje de los discos ASM es /mnt/my-asm-disks/**/disk**, después de editar ASM_DISKSTRING, la ruta actualizada es /opt/NetApp/smo/mnt/my-asm-disks-20081012/disk1.nfs. El parámetro ASM_DISKSTRING tiene el formato /opt/NetApp/smo/mnt/**/disk**.

   - El primero * coincide con my-asm-disks-20081012.
   - El disco* coincide con disk1.nfs. Después de editar el parámetro ASM_DISKSTRING, los resultados de ASM que descubre los discos importados por SnapManager son los siguientes:
   - Clon de ASM en NFS disk1 es /opt/NetApp/smo/mnt/-mnt-my-asm-disks-20081012/dir1/disk1.nfs.
   - Clon de ASM en NFS disk2 es /opt/NetApp/smo/mnt/-mnt-my-asm-disks-20081012/dir1/disk2.nfs. El parámetro ASM_DISKSTRING tiene la forma /opt/NetApp/smo/mnt//disk*.
   - El primero * coincide -mnt-my-asm-disks-20081012.
   - El segundo * coincide con dir1.
   - El tercero * coincide con disk1.nfs y disk2.nfs.
2. Si utiliza discos ASM en el entorno DE la red DE área de almacenamiento (SAN), en función del entorno realice una de las siguientes acciones:

Si utiliza discos ASM con…	Realice lo siguiente…
ASMLib sobre FCP e iSCSI en Linux	Cambie el permiso del propietario del software de Oracle y del grupo principal del usuario utilizando únicamente el dispositivo de caracteres. La ruta ASM_DISKSTRING debe ser ASM DISKSTRING = ORCL:*.
FCP e iSCSI en AIX	Añada el nombre de la ruta de acceso del parámetro ASM_DISKSTRING hasta la ruta del directorio ASM. La ruta ASM_DISKSTRING debe ser ASM DISKSTRING = /dev/hdsk/*, donde * indica el nombre del disco de ASM.
FCP e iSCSI en Solaris	Añada el nombre de la ruta de acceso del parámetro ASM_DISKSTRING hasta la ruta del directorio ASM. La ruta ASM_DISKSTRING debe ser ASM DISKSTRING = /dev/rdsk/*, donde * indica el nombre del disco ASM. +

"Documentación de Oracle: www.oracle.com/technetwork/indexes/documentation/index.html"

Seguridad y gestión de credenciales

Puede gestionar la seguridad en SnapManager aplicando la autenticación del usuario y el control de acceso basado en roles (RBAC). El método de autenticación de usuario permite acceder a recursos como repositorios, hosts y perfiles. El control de acceso basado en roles permite restringir las operaciones que SnapManager puede realizar en los volúmenes y LUN que contienen los archivos de datos de la base de datos.

Cuando se realiza una operación mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario (GUI), SnapManager recupera las credenciales establecidas para repositorios y perfiles. SnapManager guarda las credenciales de instalaciones anteriores.

El repositorio y los perfiles se pueden proteger con una contraseña. Una credencial es la contraseña configurada para el usuario de un objeto y la contraseña no está configurada en el objeto en sí.

Puede gestionar la autenticación y las credenciales realizando las siguientes tareas:

- Gestione la autenticación de usuarios mediante mensajes de contraseña en las operaciones o mediante el uso del comando smo credential set.

  Configurar credenciales para un repositorio, host o perfil.

- Vea las credenciales que rigen los recursos a los que tiene acceso.
- Borre las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Eliminar credenciales de un usuario para recursos individuales (hosts, repositorios y perfiles).

Para gestionar el acceso basado en roles, debe realizar las siguientes tareas:

- Habilite RBAC para SnapManager mediante SnapDrive.
- Asigne usuarios a las funciones y establezca las funciones mediante la consola de Operations Manager.
- De manera opcional, habilite SnapManager para almacenar contraseñas cifradas mediante la edición del archivo smo.config.

Si está instalado Protection Manager, el acceso a las funciones se ve afectado de las siguientes maneras:

- Si se instala Protection Manager, al crear un perfil de base de datos, SnapManager crea un conjunto de datos y rellena el conjunto de datos con los volúmenes que contienen los archivos de base de datos.

  Después de una operación de backup, SnapManager mantiene el contenido del conjunto de datos sincronizado con los archivos de la base de datos.

- Si Protection Manager no está instalado, SnapManager no puede crear un conjunto de datos y no podrá establecer la protección en los perfiles.

Qué es la autenticación de usuario

Además de utilizar el control de acceso basado en roles (RBAC), SnapManager autentica al usuario por medio de un inicio de sesión en el sistema operativo (SO) en el host en el que se ejecuta el servidor SnapManager. Puede habilitar la autenticación de usuario mediante mensajes de contraseña en las operaciones o mediante el comando smo credential set.

Los requisitos de autenticación de usuario dependen de dónde se realice la operación.

- Si el cliente SnapManager está en el mismo servidor que el host SnapManager, se autenticará mediante las credenciales del sistema operativo.

  No se le solicita una contraseña porque ya ha iniciado sesión en el host donde se ejecuta el servidor SnapManager.

- Si el cliente SnapManager y el servidor SnapManager están en hosts diferentes, SnapManager debe autenticarse con ambas credenciales de sistema operativo.

  SnapManager solicita contraseñas para cualquier operación si no se guardaron las credenciales del sistema operativo en la caché de credenciales del usuario SnapManager. Si introduce el comando smo credential set -host, guarde las credenciales del sistema operativo en el archivo de la caché de credenciales de SnapManager, de modo que SnapManager no solicita la contraseña de ninguna operación.

Si está autenticado con el servidor SnapManager, se considera el usuario efectivo. El usuario efectivo para cualquier operación debe ser una cuenta de usuario válida en el host donde se ejecuta la operación. Por ejemplo, si ejecuta una operación de clonado, debe poder iniciar sesión en el host de destino del clon.

> SnapManager para Oracle podría fallar al autorizar a los usuarios creados en Servicios de Active Directory central, como LDAP y ANUNCIOS. Para asegurarse de que la autenticación no falla, debe establecer auth.disableServerAuthorization configurable en true.

Como usuario eficaz, puede gestionar las credenciales de las siguientes maneras:

- De manera opcional, es posible configurar SnapManager para almacenar credenciales de usuario en el archivo de credenciales de usuario de SnapManager.

  De manera predeterminada, SnapManager no almacena las credenciales del host. Puede resultar conveniente cambiar esto, por ejemplo, si tiene scripts personalizados que requieren acceso en un host remoto. La operación de clonado remoto es un ejemplo de una operación SnapManager que necesita las credenciales de inicio de sesión de un usuario para un host remoto. Para que SnapManager recuerde las credenciales de inicio de sesión de host del usuario en la caché de credenciales de usuario de SnapManager, establezca la propiedad host.credential.persists en TRUE en el archivo smo.config.

- Puede autorizar el acceso de los usuarios al repositorio.
- Puede autorizar el acceso de los usuarios a los perfiles.
- Es posible ver todas las credenciales de usuario.
- Es posible borrar las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Es posible eliminar credenciales de recursos individuales (hosts, repositorios y perfiles).

Acerca del control de acceso basado en roles

El control de acceso basado en roles permite controlar quién tiene acceso a las operaciones de SnapManager. Con RBAC, los administradores pueden gestionar grupos de usuarios al definir roles y asignar usuarios a esos roles. Puede ser conveniente utilizar el control de acceso basado en roles de SnapManager en entornos donde ya se encuentra el control de acceso basado en roles.

El control de acceso basado en roles incluye los siguientes componentes:

- Recursos: Volúmenes y LUN que contienen los archivos de datos que componen la base de datos.
- Capabilities: Tipos de operaciones que se pueden realizar en un recurso.
- Usuarios: Personas a las que usted concede capacidades.
- Funciones: Un conjunto de recursos y capacidades que se permiten en los recursos. Asigne un rol específico a un usuario que deba realizar esas capacidades.

Es posible habilitar el control de acceso basado en roles en SnapDrive. A continuación, puede configurar capacidades específicas por función en la interfaz gráfica de usuario web o en la interfaz de línea de comandos de Operations Manager. Las comprobaciones de RBAC se realizan en DataFabric Manager Server.

En la tabla siguiente se enumeran algunas funciones y sus tareas típicas, tal como se establece en el Administrador de operaciones.

Función	Tareas típicas
Administrador de bases de datos Oracle	• Crear, mantener y supervisar una base de datos de Oracle que reside en un host • Programar y crear backups de bases de datos • Garantizar que los backups sean válidos y se puedan restaurar • Clonar bases de datos

Función	Tareas típicas
Administrador de servidores	• Configuración de sistemas de almacenamiento y agregados • Supervisar los volúmenes para obtener espacio libre • Aprovisionamiento de almacenamiento para solicitudes de usuarios • Configuración y supervisión de mirroring de recuperación de desastres
Arquitecto de almacenamiento	• Tomar decisiones sobre la arquitectura en el almacenamiento • Planificación del crecimiento de la capacidad de almacenamiento • Planificación de las estrategias de recuperación ante desastres • Delegación de capacidades a los miembros del equipo

Si está en uso RBAC (es decir, que Operations Manager está instalado y que el RBAC está habilitado en SnapDrive), el administrador de almacenamiento debe asignar permisos de RBAC en todos los volúmenes y sistemas de almacenamiento para los archivos de base de datos.

Habilitar el control de acceso basado en roles

El control de acceso basado en roles (RBAC) de SnapManager está habilitado mediante SnapDrive. Tras la instalación de SnapDrive, el control de acceso basado en roles está deshabilitado de forma predeterminada. Después de habilitar el control de acceso basado en roles en SnapDrive, SnapManager ejecuta operaciones con RBAC habilitado.

El archivo snapdrive.config en SnapDrive establece muchas opciones, una de las cuales permite RBAC.

La documentación de SnapDrive contiene detalles sobre SnapDrive.

1. Abra el archivo snapdrive.conf en un editor.
2. Habilite RBAC cambiando el valor del parámetro rbac-Method de nativo a dfm.

   El valor predeterminado para este parámetro es nativo, lo que deshabilita RBAC.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Establecimiento de funciones y funcionalidades de control de acceso basado en roles

Después de habilitar el control de acceso basado en roles (RBAC) para SnapManager mediante SnapDrive, es posible añadir funcionalidades de RBAC y usuarios a roles para ejecutar operaciones de SnapManager.

Debe crear un grupo en el servidor de Data Fabric Manager y añadir el grupo a los sistemas de almacenamiento primario y secundario. Ejecute los siguientes comandos:

- el grupo dfm crea smo_grp
- dfm group añade smo_grpprimary_storage_system
- dfm group añade smo_grpsecondary_storage_system

Es posible usar la interfaz web de Operations Manager o la interfaz de línea de comandos (CLI) del servidor de Data Fabric Manager para modificar las funcionalidades y los roles de RBAC.

En la tabla, se enumeran las capacidades de RBAC necesarias para ejecutar operaciones de SnapManager:

Operaciones de SnapManager	**Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada**	**Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada**
Creación de perfiles o actualización de perfiles	SD.Storage.Read (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile)
Protección de perfiles	DFM.Database.Write (smo_grp) SD.Storage.Read (smo_grp) SD.Config.Read (smo_grp) SD.Config.Write (smo_grp) SD.Config.Delete (smo_grp) GlobalDataProtection	Ninguno
Crear backup	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Write (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.Snapshot.Delete (conjunto de datos SMO_profile)

Operaciones de SnapManager	Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada	Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada
Creación de backup (con DBVerify)	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.snapshot.Clone (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Write (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.Snapshot.Delete (conjunto de datos SMO_profile) SD.snapshot.Clone (conjunto de datos SMO_profile)
Crear copia de seguridad (con RMAN)	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.snapshot.Clone (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Write (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.Snapshot.Delete (conjunto de datos SMO_profile) SD.snapshot.Clone (conjunto de datos SMO_profile)
Restauración de backup	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.snapshot.Clone (smo_grp) SD.Snapshot.Restore (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Write (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.Snapshot.Delete (conjunto de datos SMO_profile) SD.snapshot.Clone (conjunto de datos SMO_profile) SD.Snapshot.Restore (conjunto de datos SMO_profile)

Operaciones de SnapManager	Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada	Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada
Eliminación de copia de seguridad	SD.Snapshot.Delete (smo_grp)	SD.Snapshot.Delete (conjunto de datos SMO_profile)
Verificación de backup	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.Snapshot.Clone (conjunto de datos SMO_profile)
Montaje de backup	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.Snapshot.Clone (conjunto de datos SMO_profile)
Desmontaje de backups	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (conjunto de datos SMO_profile)
Clone create	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.snapshot.Clone (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.snapshot.Clone (conjunto de datos SMO_profile)
Clonar eliminación	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (conjunto de datos SMO_profile)

Operaciones de SnapManager	Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada	Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada
División de clones	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.snapshot.Clone (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Storage.Write (smo_grp)	SD.Storage.Read (conjunto de datos SMO_profile) SD.Snapshot.Read (conjunto de datos SMO_profile) SD.snapshot.Clone (conjunto de datos SMO_profile) SD.Snapshot.Delete (conjunto de datos SMO_profile) SD.Storage.Write (conjunto de datos SMO_profile)

Para obtener detalles sobre la definición de las funcionalidades de RBAC, consulte la *Guía de administración del gestor de operaciones de Unified Manager de OnCommand*.

1. Acceda a la consola de Operations Manager.
2. En el menú Configuración, seleccione **roles**.
3. Seleccione un rol existente o cree uno nuevo.
4. Para asignar operaciones a los recursos de almacenamiento de la base de datos, haga clic en **Agregar capacidades**.
5. En la página Editar configuración de función, para guardar los cambios realizados en la función, haga clic en **Actualizar**.

Información relacionada

"*OnCommand Unified Manager Operations Manager Administration Guide*: mysupport.netapp.com/documentation/productsatoz/index.html"

Almacenamiento de contraseñas cifradas para secuencias de comandos personalizadas

De forma predeterminada, SnapManager no almacena credenciales de host en la caché de credenciales de usuario. Sin embargo, puede cambiar esto. Puede editar el archivo smo.config para permitir el almacenamiento de las credenciales de host.

El archivo smo.config está ubicado en <default installation location>/properties/smo.config

1. Edite el archivo smo.config.
2. Configure host.credenciales.persista en TRUE.

Autorizando el acceso al repositorio

Además del control de acceso basado en roles (RBAC), SnapManager permite configurar credenciales para que los usuarios de la base de datos accedan al repositorio. Con las credenciales, puede restringir o evitar el acceso a hosts, repositorios, perfiles y bases de datos de SnapManager.

Si ha configurado las credenciales con el comando set de credenciales, SnapManager no le solicita una contraseña.

Es posible configurar credenciales de usuario al instalar SnapManager o una versión posterior.

1. Introduzca el siguiente comando:

   'conjunto de credenciales de meses -repository -dbname repo_service_name -host repo_host -login -username repo_username [-password repo_password] -port repo_port'

Autorizando el acceso a los perfiles

Además del control de acceso basado en roles (RBAC), SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

1. Introduzca el siguiente comando: 'Mmo credential set -profile -name profile_name [-password]'

Información relacionada

El comando smo credential set

Visualización de las credenciales de usuario

Puede enumerar los hosts, perfiles y repositorios a los que tiene acceso.

1. Para enumerar los recursos a los que tiene acceso, escriba este comando: `smo credential list`

Ejemplo de visualización de credenciales de usuario

En este ejemplo, se muestran los recursos a los que tiene acceso.

```
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
```

Información relacionada

El comando smo credential list

Borrar credenciales de usuario para todos los hosts, repositorios y perfiles

Puede borrar la caché de sus credenciales para recursos (hosts, repositorios y perfiles). Esto elimina todas las credenciales de recursos del usuario que ejecuta el comando. Después de borrar la caché, debe volver a autenticar las credenciales para obtener acceso a estos recursos protegidos.

1. Para borrar sus credenciales, introduzca el comando smo credential clear en la CLI de SnapManager o seleccione **Admin** > **credenciales** > **Clear Cache** en la GUI de SnapManager.
2. Salga de la interfaz gráfica de usuario de SnapManager.

   NOTA:

   - Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager.
   - Si borró la caché de credenciales de la interfaz de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager.
   - Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar de nuevo la interfaz gráfica de usuario de SnapManager.
3. Para volver a configurar las credenciales, repita el proceso con el fin de establecer las credenciales para el repositorio, el host del perfil y el perfil. Para obtener información adicional sobre cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales tras borrar caché de credenciales".

Información relacionada

El comando smo credential clear

Configuración de credenciales después de borrar la caché de credenciales

Después de borrar la caché para quitar las credenciales de usuario almacenadas, puede

configurar las credenciales para hosts, repositorios y perfiles.

Debe asegurarse de establecer las mismas credenciales de usuario para el repositorio, el host del perfil y el perfil que había especificado anteriormente. Se crea un archivo de credenciales cifrado al configurar las credenciales de usuario.

El archivo de credenciales está ubicado en /root/.netapp/smo/3.3.0.

Desde la interfaz gráfica de usuario (GUI) de SnapManager, si no hay ningún repositorio en repositorios, realice los siguientes pasos:

1. Haga clic en **tareas** > **Agregar repositorio existente** para agregar un repositorio existente.
2. Ejecute los siguientes pasos para configurar las credenciales del repositorio:
   a. Haga clic con el botón derecho del ratón en el repositorio y seleccione **Abrir**.
   b. En la ventana Repository Credentials Authentication, introduzca las credenciales de usuario.
3. Realice los siguientes pasos para configurar las credenciales del host:
   a. Haga clic con el botón derecho del ratón en el host bajo el repositorio y seleccione **Abrir**.
   b. En la ventana Host Credentials Authentication, introduzca las credenciales de usuario.
4. Realice los siguientes pasos para configurar las credenciales del perfil:
   a. Haga clic con el botón derecho del ratón en el perfil bajo el host y seleccione **Abrir**.
   b. En la ventana Profile Credentials Authentication, introduzca las credenciales de usuario.

Eliminación de credenciales para recursos individuales

Puede eliminar las credenciales de uno de los recursos protegidos, como un perfil, un repositorio o un host. De este modo, puede quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario de todos los recursos.

Información relacionada

El comando smo credential delete

Eliminación de credenciales de usuario para repositorios

Es posible eliminar las credenciales para que un usuario ya no pueda acceder a un repositorio en particular. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario para todos los recursos.

1. Para eliminar las credenciales de repositorio de un usuario, introduzca este comando: 'Credencial mmo delete -repository-dbnamerepo_service_name-hotrepo_host-login -usernamerepo_username -portrepo_Port'

Eliminación de credenciales de usuario para hosts

Es posible eliminar las credenciales de un host para que un usuario ya no pueda acceder a él. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar todas las credenciales del usuario para todos los recursos.

1. Para eliminar las credenciales de host de un usuario, introduzca el siguiente comando: 'Mo credential delete -host-namehost_name-username-username'

Eliminación de credenciales de usuario para perfiles

Es posible eliminar las credenciales de usuario de un perfil para que un usuario ya no pueda acceder a él.

1. Para eliminar las credenciales de perfil de un usuario, introduzca este comando: 'Mmo credential delete -profile-nameprofile_name'

Gestionar perfiles para backups eficientes

Debe crear un perfil en SnapManager para la base de datos donde desea realizar una operación. Debe seleccionar el perfil y, a continuación, seleccionar la operación que desea realizar.

Tareas relacionadas con perfiles

Es posible realizar las siguientes tareas:

- Cree perfiles para permitir backups completos o parciales y backups en almacenamiento primario, secundario o incluso terciario.

  También es posible crear perfiles para separar los backups de registros de archivo de los backups de archivos de datos.

- Verificar perfiles.
- Actualizar perfiles.
- Eliminar perfiles.

Acerca de los perfiles y la autenticación

Al crear un perfil, puede especificar una base de datos y elegir uno de los siguientes métodos para conectarse a la base de datos:

- Autenticación de Oracle con un nombre de usuario, contraseña y puerto
- Autenticación del sistema operativo (SO) sin nombre de usuario, contraseña ni puerto.

  Para la autenticación del sistema operativo, debe introducir la información de usuario y del grupo de cuenta del sistema operativo.

  > Para utilizar la autenticación del sistema operativo para las bases de datos de Real Application Cluster (RAC), el servidor SnapManager debe estar en ejecución en cada nodo del entorno RAC y la contraseña de la base de datos debe ser la misma para todas las instancias de Oracle de un entorno RAC. SnapManager utiliza el nombre de usuario y la contraseña de la base de datos para conectarse a cada instancia de RAC del perfil.

- Autenticación de base de datos cuando sqlnet.authentication_services está establecido en NONE. A continuación, SnapManager utiliza el nombre de usuario y la contraseña de la base de datos para todas las conexiones con la base de datos de destino.

Para utilizar la autenticación de la base de datos para una instancia de Automatic Storage Management (ASM), se debe introducir el nombre de usuario y la contraseña que se utilizan para iniciar sesión en la instancia de ASM.

Puede establecer sqlnet.authentication_services a NINGUNO solo en los siguientes entornos:

Distribución de la base de datos	Versión de Oracle	Es compatible con la autenticación de la base de datos de destino	Es compatible con la autenticación de base de datos para la instancia de ASM
Cualquier base de datos que no sea ASM y que no sea RAC	Oracle 10g y Oracle 11g (inferior a 11.2.0.3)	Sí	No
Base de datos ASM independiente en UNIX	Oracle 11.2.0.3 y posterior	Sí	Sí
Instancia de ASM en base de datos RAC en UNIX	Oracle 11.2.0.3	No	No
Base de datos RAC en NFS	Oracle 11.2.0.3	Sí	No

Nota: después de deshabilitar sqlnet.authentication_services y cambiar el método de autenticación a autenticación de base de datos, debe establecer sqlnet.authentication_services en NINGUNO.

Si accede a un perfil por primera vez, debe introducir la contraseña de su perfil. Después de introducir sus credenciales, es posible ver los backups de la base de datos dentro del perfil.

Información relacionada

Qué perfiles son

Creación de perfiles

Al crear perfiles, puede asignar una cuenta de usuario de base de datos Oracle concreta al perfil. Puede establecer la política de retención para el perfil, habilitar la protección de backup en el almacenamiento secundario para todos los backups mediante este perfil, y establecer el número de retención y la duración de cada clase de retención.

Si no se proporcionan los valores de los parámetros -login, -password y -Port de la base de datos, el modo de autenticación del sistema operativo utiliza las credenciales predeterminadas.

Al crear un perfil, SnapManager realiza una comprobación de elegibilidad de restauración para determinar el mecanismo de restauración que puede usarse para restaurar la base de datos. Si la base de datos se encuentra en un qtree y el volumen principal no es apto para una restauración rápida o basada en el volumen, es posible que el análisis no se realice correctamente.

SnapManager (3.2 o posterior) permite separar los archivos de registro de archivos de los archivos de datos al crear un nuevo perfil o actualizar un perfil existente. Después de separar el backup con el perfil, se puede

crear únicamente el backup de los archivos de datos o el backup de solo registro del archivo de la base de datos. Se puede usar el nuevo perfil o el perfil actualizado para crear el backup que contiene tanto los archivos de datos como los archivos de registro de archivos. Sin embargo, no se puede utilizar el perfil para crear el backup completo ni revertir la configuración.

Perfiles para crear copias de seguridad completas y parciales

Es posible crear perfiles para crear un backup completo de la base de datos que contenga los archivos de datos, los archivos de control, los archivos de registro de archivos y el backup parcial de la base de datos que contenga los archivos de datos o espacios de tablas especificados, todos los archivos de control y todos los archivos de registro de archivos. SnapManager no permite crear backups de registros de archivos independientes con los perfiles creados para backups completos y parciales.

Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad sólo archivogs

Al crear un nuevo perfil, puede incluir -separate-archivvelog-backups para separar el backup del registro de archivo del backup del archivo de datos. También puede actualizar el perfil existente para separar la copia de seguridad del archivo de datos.

Al usar las opciones nuevas de perfil para separar los backups de los registros de archivos, es posible realizar las siguientes operaciones de SnapManager:

- Cree un backup de registro de archivos
- Eliminar un backup de registro de archivos
- Montar un backup de registro de archivos
- Liberar un backup de registro de archivo

Al crear el perfil para separar los backups de registros de archivos del backup de archivos de datos, si los archivos de registro de archivos no existen en la base de datos para la que se creó el perfil, no existe un archivo de registro archivado con mensaje de advertencia en el sistema de archivos activo. Las versiones del archivo de registro archivado anteriores al archivo de registro de <archive log thread version> no se incluirán en el backup. Incluso si se crean backups para esta base de datos, los archivos de registro de archivos no están disponibles en los backups de la base de datos.

> Si se produce un error al crear un perfil, utilice el comando smosystem dump. Después de crear un perfil, si se encuentra con un error, utilice los comandos dump y smofrofile dump de operación.

1. Para crear un perfil con un nombre de usuario, una contraseña y un puerto (autenticación de Oracle), introduzca el comando siguiente: 'Mmo-profile create -profileprofile [-profile-passwordprofile_password] -repository [-dbnamerepo_dbnombrecompensode[-nombredeusuario] [-nombredeusuario-nombredeusuario] [-nombredeusuario_nombredeusuario] [-nombredeusuario_nombredeusuario] [-nombredeusuario_nombredeusuario]-nombredeusuario_nombredeusuario] [-nombredeusuario_nombredeusuario_nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario-nombredearchivo-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario]

Las demás opciones para este comando son las siguientes:

'[-force] [-noprompt]'

'[silencio | detallado]'

> Para entornos RAC, al crear un nuevo perfil, debe proporcionar el valor del parámetro dB_UNIQUE_NAME como dB_dbname.

También puede incluir otras opciones al crear perfiles, dependiendo de cómo desee tener acceso a la base de datos.

Si…	Realice lo siguiente…
Desea utilizar la autenticación del sistema operativo para crear el perfil	Especifique las variables para una cuenta de sistema operativo en el grupo DBA (normalmente la cuenta utilizada para instalar Oracle). En lugar de agregar el nombre de usuario, la contraseña y el puerto, especifique lo siguiente: • -osaccountaccount_name como el nombre de la cuenta del sistema operativo • -osgruposgrupo como grupo asociado a la cuenta del sistema operativo
Desea utilizar la autenticación de instancia de Automatic Storage Management (ASM) para crear el perfil	Especifique las credenciales para la autenticación de instancias de ASM. • -Asmusernameasminance_username es el nombre de usuario utilizado para iniciar sesión en la instancia de ASM. • -Asmpaswordasminstance_password es la contraseña utilizada para iniciar sesión en la instancia de ASM.
Desea utilizar la autenticación de base de datos para crear un perfil	Especifique los detalles de inicio de sesión de la base de datos. Si la contraseña contiene caracteres especiales como el signo de exclamación (!), el signo de dólar ($) o el acento grave ('), SnapManager no permite crear el perfil autenticado de la base de datos desde la interfaz de línea de comandos (CLI).

Está utilizando un catálogo como repositorio de Oracle Recovery Manager (RMAN)	Especifique las siguientes opciones y variables: • -tnsnametnsname como el tnsname definido en el archivo tnsnames.ora. • -Login -usernameusername como el nombre de usuario requerido para conectarse al catálogo de RMAN. Si no se especifica, SnapManager utiliza la información de autenticación del sistema operativo. No se puede usar la autenticación del sistema operativo con bases de datos RAC. • -Passwordpassword como contraseña de RMAN requerida para conectarse al catálogo de RMAN.
Está utilizando el archivo de control como repositorio de RMAN	Especifique la opción -Controlfile.
Desea especificar una política de retención de copias de seguridad para copias de seguridad	Especifique el recuento de retención o la duración de una clase de retención, o ambos. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). • -hourly es la clase de retención por hora, para la cual [-count n] [-duration m] son el recuento de retención y la duración de la retención, respectivamente. • -daily es la clase de retención diaria, para la cual [-count n] [-durationm] son el recuento de retención y la duración de la retención, respectivamente. • -weekly es la clase de retención semanal, para la cual [-count n] [-duration m] son el recuento de retención y la duración de la retención, respectivamente. • -monthly es la clase de retención mensual, para la cual [-count n] [-durationm] son el recuento de retención y la duración de la retención, respectivamente.

Desea activar la protección de copia de seguridad para el perfil	Especifique las siguientes opciones y variables: • -protect permite la protección de copia de seguridad. Si utiliza Data ONTAP funcionando en 7-Mode, esta opción crea un conjunto de datos de aplicación en el servidor de Data Fabric Manager (DFM) y añade miembros relacionados con la base de datos, los archivos de datos, los archivos de control y los registros de archivos. Si el conjunto de datos ya existe, se vuelve a utilizar el mismo conjunto de datos cuando se crea un perfil. • -política de protección permite especificar la política de protección. Si se usa Data ONTAP en 7-Mode y SnapManager se integra con Protection Manager, es necesario especificar una de las políticas de Protection Manager. Para enumerar las posibles políticas de protección, use el comando smo protection-policies list. Si utiliza Clustered Data ONTAP, debe seleccionar *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault*. Se produce un error en la operación de creación de perfiles en las siguientes situaciones: ◦ Si utiliza Clustered Data ONTAP, pero seleccione Protection Manager policy ◦ Si utiliza Data ONTAP operando en 7-Mode, pero seleccione la política de *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault* ◦ Si creó la relación de SnapMirror pero seleccionó *SnapManager_CDOT_Vault* o creó la relación de SnapVault, pero seleccionó la política *SnapManager_CDOT_Mirror* ◦ Si no ha creado la relación de SnapMirror o SnapVault, pero ha seleccionado la política *SnapManager_CDOT_Vault* o *SnapManager_CDOT_Mirror* • -noprotect indica que no es necesario proteger las copias de seguridad de la base de datos creadas con el perfil. **Nota:** Si se especifica -Protect sin -protection-policy, el dataset no

Desea activar la notificación por correo electrónico para el estado de finalización de las operaciones de la base de datos	Especifique las siguientes opciones y variables: • -summary-notification permite configurar una notificación de correo electrónico de resumen para varios perfiles en una base de datos de repositorio. • -notification permite recibir una notificación por correo electrónico del estado de finalización de la operación de base de datos de un perfil. • -success-emailemail_address2 le permite recibir una notificación por correo electrónico sobre la operación correcta de la base de datos mediante un perfil nuevo o existente. • -failure-emailemail_address2 le permite recibir una notificación por correo electrónico sobre la operación de la base de datos fallida realizada mediante un perfil nuevo o existente. • -subjectsubject_text especifica el texto del asunto para la notificación de correo electrónico al crear un perfil nuevo o uno existente. Si los ajustes de notificación no están configurados para el repositorio y intenta configurar las notificaciones de perfil o resumen mediante la CLI, se registra el siguiente mensaje en el registro de consola: 'MO-14577: Ajustes de notificación no configurados'. Si ha configurado la configuración de notificación e intenta configurar la notificación de resumen mediante la CLI sin habilitar la notificación de resumen para el repositorio, se muestra el siguiente mensaje en el registro de consola: 'MO-14575: Configuración de notificación de resumen no disponible para este repositorio**'

Desea hacer una copia de seguridad de los archivos de registro de archivos por separado de los archivos de datos	Especifique las siguientes opciones y variables: • -separar-archivvelog-backups permite separar el backup de registros de archivo del backup del archivo de datos. • -retain-archivvelog-backups establece la duración de la retención para los backups de registros de archivos. Debe especificar una duración de retención positiva. Los backups de los registros de archivos se conservan según la duración de retención de los registros de archivo. Los backups de los archivos de datos se retienen en función de las políticas de retención existentes. • -protect permite proteger los backups de registros de archivos. • -protection-policy establece la política de protección en los backups de registros de archivos. Los backups de registros de archivos se protegen de acuerdo con la política de protección de registros de archivos. Los backups de los archivos de datos se protegen de acuerdo con las políticas de protección existentes. • -include-with-online-backups incluye el backup de registros de archivos junto con el backup de base de datos en línea. Esta opción permite crear un backup de archivos de datos en línea y un backup de registros de archivos juntos para el clonado. Cuando se configura esta opción, siempre que se crea un backup de archivos de datos en línea, se crean los backups de los registros de archivos junto con los archivos de datos inmediatamente. • -no-include-with-online-backups no incluye el backup de registros de archivo junto con el backup de base de datos.
Puede recopilar los archivos de volcado después de que la operación de creación de perfil se haya realizado correctamente	Especifique la opción -dump al final del comando profile create.

Cuando se crea un perfil, SnapManager analiza los archivos en caso de que posteriormente se desee realizar una operación de restauración basada en volumen en los archivos especificados en el perfil.

Información relacionada

Cómo recopilar archivos de volcado

Nomenclatura de copias Snapshot

Puede especificar una convención o un patrón de nomenclatura para describir las copias de Snapshot relacionadas con el perfil que crea o actualiza. También puede incluir texto personalizado en todos los nombres de copias de Snapshot.

Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias Snapshot que todavía no se han producido; las copias Snapshot que existen conservan el patrón de snapname anterior.

Los siguientes ejemplos muestran los dos nombres de copias Snapshot tomados de un volumen. La segunda copia snapshot que se muestra tiene *F_H_1* en la mitad de su nombre. El "1" indica que es la primera copia snapshot tomada en el conjunto de backup. La primera copia Snapshot enumerada es la más reciente y tiene una «2», lo que significa que se toma la segunda copia Snapshot. La copia Snapshot "1" incluye los archivos de datos; la copia Snapshot "2" incluye los archivos de control. Dado que las copias snapshot del archivo de control deben realizarse después de realizar la copia snapshot del archivo de datos, se necesitan dos copias snapshot.

```
smo_profile_sid_f_h_2_8ae482831ad14311011ad14328b80001_0
smo_profile_sid_f_h_1_8ae482831ad14311011ad14328b80001_0
```

El patrón predeterminado incluye el smid requerido, como se muestra en la siguiente:

'* patrón predeterminado: smo_{perfil}_{dB-sid}_{ámbito}_{modo}_{mitad} * ejemplo: smo_my_profile_rac51_f_h_2_8abc01e915a55ac50115a55acc8d0001_0'

Es posible usar las siguientes variables en el nombre de la copia Snapshot:

Nombre de la variable	Descripción	Valor de ejemplo
smid (obligatorio)	El ID único de SnapManager es el único elemento requerido cuando se crea un nombre para la copia Snapshot. Este ID garantiza la creación de un nombre de snapshot único.	8abc01e915a55ac50115a55ac8d0001_0
Clase (opcional)	Clase de retención asociada al backup para el perfil e indicada por cada hora (h), día (d), semanal (w), mensual (m) o ilimitado (u).	d

Comentario (opcional)	Comentario asociado al backup del perfil. Los espacios en este campo se convertirán en guiones bajos cuando se complete el nombre de la copia Snapshot.	sample_comment_spaces_reemplazado
Fecha (opcional)	Fecha en la que se realiza la copia de seguridad para el perfil. Los valores de fecha se rellenarán con ceros si es necesario. (aaaammdd)	20070218
db-host (opcional)	Nombre de host de la base de datos asociado con el perfil que se va a crear o actualizar.	mi_host
db-name (opcional)	Nombre de la base de datos asociada con la copia de Snapshot que crea.	rac5
db-sid (opcional)	sid de base de datos asociado con la copia de Snapshot que crea.	racer51
Etiqueta (opcional)	Etiqueta asociada al backup para el perfil.	etiqueta_muestra
Modo (opcional)	Especifica si el backup se completa en línea (h) o sin conexión (c).	h
Perfil (opcional)	El nombre del perfil asociado con el backup que cree.	mi_perfil
Alcance (opcional)	Especifica si el backup está completo (f) o parcial (p).	f
Tiempo (opcional)	Hora a la que se produce el backup para el perfil. Los valores de hora de esta variable utilizan el reloj de 24 horas y están acolchados con ceros si es necesario. Por ejemplo, 5:32 y 8 segundos se muestran como 053208 (hhmmss).	170530
Zona horaria (opcional)	Zona horaria especificada para el host de la base de datos de destino.	EST
Usertext (opcional)	Texto personalizado que puede introducir.	prod

Nota: SnapManager para Oracle no admite el símbolo de dos puntos (:) en las formas largas de los nombres de las copias Snapshot.

Cambiar el nombre de los perfiles

SnapManager le permite cambiar el nombre del perfil al actualizar el perfil. Las funcionalidades de SnapManager establecidas en el perfil y las operaciones que se pueden realizar antes de cambiar de nombre se conservan para el perfil cuyo nombre ha cambiado.

- Debe asegurarse de que no haya operaciones SnapManager en ejecución en el perfil mientras cambia el nombre del perfil.

Es posible cambiar el nombre del perfil tanto en la interfaz de línea de comandos (CLI) de SnapManager como en la interfaz gráfica de usuario (GUI). Al actualizar el perfil, SnapManager verifica y actualiza el nombre del perfil en el repositorio.

> SnapManager no admite cambiar el nombre del perfil en la ventana de actualización de varios perfiles.

Cuando proporcione un nuevo nombre de perfil, el nuevo nombre de perfil se añadirá a la caché de credenciales del cliente y se eliminará el nombre del perfil anterior. Al cambiar el nombre del perfil desde un cliente, sólo se actualiza la caché de credenciales de ese cliente. Debe ejecutar el comando smo profile SYNC desde cada cliente para actualizar la nueva caché de credenciales con el nombre del nuevo perfil.

Puede establecer la contraseña del perfil mediante el comando smo credential set.

Si se incluyó el nombre de perfil en un patrón de nomenclatura de copias Snapshot, al cambiar el nombre de un perfil, se actualiza el nuevo nombre del perfil. Todas las operaciones SnapManager que se realizan en el perfil utilizan el nuevo nombre del perfil. Los backups creados con el perfil anterior siguen teniendo el nombre del perfil anterior y se usan para realizar otras operaciones de SnapManager.

Si va a realizar la actualización gradual de los hosts del servidor SnapManager, debe asegurarse de realizar la actualización completa antes de cambiar el nombre del perfil.

El nuevo nombre del perfil sólo se actualiza desde el cliente SnapManager desde el que se realiza la solicitud. Los clientes SnapManager conectados al servidor SnapManager no reciben notificaciones sobre el cambio en el nombre del perfil. Puede comprobar el registro de operaciones para conocer el cambio en el nombre del perfil.

> Si una operación de backup programada comienza en el momento de cambiar el perfil, entonces se produce un error en la operación programada.

1. Introduzca el siguiente comando: "Mo profile update -profileprofile [-new-profilenew_profile_name]"

Cambio de contraseñas de perfil

Para proteger los perfiles existentes en el repositorio, debe actualizar las contraseñas de los perfiles. Puede aplicar esta contraseña actualizada al crear una copia de seguridad con este perfil.

1. Para actualizar la contraseña de perfil de un perfil existente, escriba este comando:

'mmo profile update -profile_name -profile-password'

Información relacionada

El comando smo profile update

Restablecimiento de la contraseña del perfil

Puede restablecer la contraseña del perfil si no recuerda la contraseña que ha proporcionado al crear el perfil.

- Debe asegurarse de que el servidor SnapManager esté en ejecución en la base de datos del repositorio.
- Debe tener las credenciales de usuario raíz del host en el que reside la base de datos del repositorio.
- Debe asegurarse de que el perfil no esté en uso para ninguna operación cuando se restablezca la contraseña para ese perfil.

Puede restablecer la contraseña desde la interfaz de línea de comandos o desde la interfaz gráfica de usuario de SnapManager. Al restablecer la contraseña, SnapManager consulta al servidor SnapManager en el host de repositorios para identificar el sistema operativo para el host de repositorios. Debe introducir las credenciales de usuario autorizado para conectarse con el host de repositorios. El servidor SnapManager autentica a los usuarios con sus credenciales de raíz en la base de datos de repositorios. Cuando la autenticación se realiza correctamente, SnapManager restablece la contraseña del perfil en el servidor SnapManager con la nueva contraseña.

SnapManager no mantiene el historial de las operaciones de restablecimiento de contraseña.

1. Restablezca la contraseña de perfil. Para ello, introduzca el siguiente comando: 'Mo password reset -profeprofile [-profile-passwordprofile_password] [-Repository-hostadmin-passwordadmin_password]'

Autorizando el acceso a los perfiles

Además del control de acceso basado en roles (RBAC), SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

1. Introduzca el siguiente comando: 'Mmo credential set -profile -name profile_name [-password]'

Información relacionada

El comando smo credential set

Verificando perfiles

Puede comprobar que un perfil existente está configurado correctamente. Cuando se verifica un perfil, SnapManager comprueba si el entorno del perfil que se ha especificado y verifica que el perfil está configurado y que la base de datos de este perfil esté accesible.

1. Para verificar si el perfil está configurado correctamente, escriba el siguiente comando: `smo profile verify -profile profile_name`

Información relacionada

El comando smo profile verify

Actualizando perfiles

Puede actualizar los perfiles para modificar la contraseña del perfil, la cantidad de backups que se deben retener, el acceso a la base de datos, la autenticación del sistema operativo (SO) con la autenticación de la base de datos y viceversa, e información sobre el host. Si cambia la información de contraseña de la base de datos Oracle, también debe cambiar esa información en el perfil.

Si la política de protección está habilitada en el perfil, no podrá cambiar la política mediante SnapManager. El administrador de almacenamiento debe cambiar la política mediante la consola de Protection Manager.

SnapManager (3.2 o posterior) permite actualizar el perfil para separar los backups de registros de archivos de los backups de archivos de datos con la opción -separate-archivvelog-backups. Es posible especificar una duración de retención y una política de protección separadas para el backup de registros de archivos. SnapManager le permite incluir el backup de registros de archivos junto con el backup de base de datos en línea. También puede crear un backup de archivo de datos en línea y un backup de registro de archivo juntos para clonar. Cuando se crea un backup de archivos de datos en línea, los backups de registros de archivos se crean inmediatamente junto con los archivos de datos.

1. Introduzca el siguiente comando: `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]`

   Las demás opciones para este comando son las siguientes:

   [-force] [-noprompt]

Si desea…	Realice lo siguiente…
Cambie el perfil para utilizar la autenticación del sistema operativo	En lugar de agregar el nombre de usuario, la contraseña y el puerto, especifique lo siguiente: • -osaccountaccount_name como el nombre de la cuenta del sistema operativo • -Osgruposgroup como el grupo asociado a la cuenta del sistema operativo, normalmente la cuenta utilizada para instalar Oracle
Utilice la autenticación de instancia de Automatic Storage Management (ASM) para crear el perfil	Especifique las credenciales para la autenticación de instancias de ASM. • -Asmusernameasminstance_username es el nombre de usuario utilizado para iniciar sesión en la instancia de ASM. • -Asmpaswordasminstance_password es la contraseña utilizada para iniciar sesión en la instancia de ASM.
Utilice un catálogo como repositorio de Oracle Recovery Manager (RMAN) o elimine RMAN	Especifique las siguientes opciones y variables: • -tnsname tnsname como el tnsname definido en el archivo tnsnames.ora. • -Login -username como el nombre de usuario requerido para conectarse al catálogo de RMAN. Si no se especifica, SnapManager utiliza la información de autenticación del sistema operativo. No se puede utilizar la autenticación del sistema operativo con bases de datos de Real Application Clusters (RAC). • -Passwordpassword como contraseña de RMAN requerida para conectarse al catálogo de RMAN. • -Controlfile si utiliza el archivo de control como repositorio de RMAN. • -Remove-rman para quitar RMAN.

Si desea…	Realice lo siguiente…
Cambiar la política de retención de copias de seguridad para copias de seguridad de la base de datos en el perfil	Especifique el recuento de retención o la duración de la retención para una clase de retención, o ambos, para cambiar la política de retención. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). • -hourly es la clase de retención por hora, para la que [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente. • -daily es la clase de retención diaria, para la cual [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente. • -weekly es la clase de retención semanal, para la cual [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente. • -mensual es la clase de retención mensual, para la que [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente.
Desactive la protección de copia de seguridad para el perfil	Especifique -noProtect para no proteger los backups de la base de datos creados mediante el perfil. En el caso de un perfil que tenga -Protect habilitado, si desea desactivar Protect, aparecerá un mensaje de advertencia que indique que esta acción eliminará el conjunto de datos y no podrá restaurar o clonar backups para este perfil.

Si desea…	Realice lo siguiente…
Activar notificaciones por correo electrónico para el estado de finalización de las operaciones de la base de datos	Especifique las siguientes opciones y variables: • -summary-notification permite configurar una notificación de correo electrónico de resumen para varios perfiles en una base de datos de repositorio. • -notification permite recibir una notificación por correo electrónico sobre el estado de finalización de la operación de base de datos de un perfil. • -success-emailemail_dirección2 le permite recibir una notificación por correo electrónico tras la finalización de una operación de base de datos exitosa usando un perfil nuevo o existente. • -failure-emailemail_address2 le permite recibir una notificación por correo electrónico en una operación de base de datos fallida realizada mediante un perfil nuevo o existente. • -subjectsubject_text especifica el texto del asunto para la notificación de correo electrónico mientras se crea un perfil nuevo o un perfil existente. Si los ajustes de notificación no están configurados para el repositorio y intenta configurar las notificaciones de perfil o resumen mediante la interfaz de línea de comandos (CLI), se registra el siguiente mensaje en el registro de consola: SMO-14577: Notification Settings not configured. Si ha configurado la configuración de notificación y está intentando configurar la notificación de resumen utilizando la CLI sin habilitar la notificación de resumen para el repositorio, se registra el siguiente mensaje en el registro de consola: SMO-14575: Configuración de notificación de resumen no disponible para este repositorio_**

Si desea…	Realice lo siguiente…
Actualice el perfil para crear una copia de seguridad de los archivos de registro de archivos por separado	Especifique las siguientes opciones y variables: • -separate-archivvelog-backups permite crear una copia de seguridad de los archivos de registro de archivos por separado de los archivos de la base de datos. Después de especificar esta opción, puede crear una copia de seguridad sólo de archivos de datos o una copia de seguridad sólo de archivvelogs. No es posible crear un backup completo. Además, no puede revertir la configuración del perfil separando la copia de seguridad. SnapManager conserva los backups según la política de retención de los backups que se crearon antes de usar un backup de solo archivado. • -retain-archivvelog-backups establece la duración de la retención para los backups de registros de archivos. Si actualiza el perfil por primera vez, puede separar los backups de registros de archivos del backup de archivos de datos con la opción -separate-archivvelog -backups; debe proporcionar la duración de retención para los backups de registros de archivos mediante la opción -retain -archivvelog-backups. La configuración de la duración de la retención es opcional cuando se actualiza el perfil más adelante. • -Protect crea un conjunto de datos de aplicaciones en el servidor Data Fabric Manager (DFM) y añade miembros relacionados con la base de datos, los archivos de datos, los archivos de control y los registros de archivos. Si el conjunto de datos existe, se vuelve a utilizar cuando se crea un perfil. • -protection-policy establece la política de protección en los backups de registros de archivos. • -include-with-online-backups especifica que el backup de registros de archivos se incluye junto con el backup de base de datos. -no-include-with-online-backups especifica el backup del archivo de registro de archivos no

Si desea…	Realice lo siguiente…
Cambiar el nombre de host de la base de datos de destino	Especifique -hostnew_dB_host para cambiar el nombre de host del perfil.
Recopilar los archivos de volcado después de la operación de actualización de perfil	Especifique la opción -dump.

2. Para ver el perfil actualizado, escriba el comando siguiente: `smo profile show`

Información relacionada

Cómo recopilar archivos de volcado

Eliminar perfiles

Puede eliminar un perfil en cualquier momento, siempre que no contenga copias de seguridad correctas o incompletas. Es posible eliminar perfiles que contengan copias de seguridad liberadas o eliminadas.

1. Para eliminar un perfil, escriba este comando: `smo profile delete -profile profile_name`

Información relacionada

El comando smo profile delete

Realizar backups de bases de datos

SnapManager permite realizar backups de datos en recursos de almacenamiento local mediante un scriptsor de posprocesamiento gracias a la protección de backups en recursos de almacenamiento secundarios o terciarios. La opción de realizar backups en el almacenamiento secundario proporciona una capa adicional que conserva los datos en caso de desastre.

SnapManager también permite a los administradores de almacenamiento configurar sus backups según sus planes de normativas. Mediante el uso de SnapManager, los administradores pueden identificar backups que no cumplan con los requisitos de las normativas y rectificarlos de inmediato.

SnapManager ofrece las siguientes opciones para realizar backups, restaurar y recuperar los datos de la base de datos:

- Realice una copia de seguridad de toda la base de datos o de una parte de ella.

  Si realiza una copia de seguridad de una parte de la misma, especifique un grupo de tablespaces o un grupo de archivos de datos.

- Realice una copia de seguridad de los archivos de datos y de los archivos de registro de archivo por separado.
- Realice un backup de las bases de datos en el almacenamiento primario (también llamado almacenamiento local) y protéjalas al realizar un backup en un almacenamiento secundario o terciario

(también llamado almacenamiento remoto).

- Programar copias de seguridad rutinarias.

La diferencia entre SnapManager (3.2 o posterior) y las versiones anteriores de SnapManager

SnapManager (3.1 o anterior) permite crear backups completos de la base de datos que contienen archivos de datos, archivos de control y archivos de registro de archivos.

SnapManager (3.1 o anterior) solo administra los archivos de datos. Los archivos de registro de archivos se mantienen usando soluciones fuera de SnapManager.

SnapManager (3.1 o anterior) impone las siguientes restricciones en la gestión de los backups de las bases de datos:

- Impacto en el rendimiento

  Cuando se realiza un backup de base de datos en línea completo (cuando la base de datos está en modo de backup), el rendimiento de la base de datos se reduce durante el periodo de tiempo hasta que se crea el backup. En SnapManager (3.2 o posterior), pueden realizarse backups de bases de datos limitados y backups frecuentes de registros de archivo. La realización de backups frecuentes de registros de archivos ayuda a evitar que la base de datos se coloque en modo de backup.

- Restauración y recuperación manuales

  Cuando los archivos de registro de archivos necesarios no existen en el sistema de archivos activo, los administradores de la base de datos deben identificar qué backup contiene los archivos de registro de archivos, montar los backups de la base de datos y recuperar la base de datos restaurada. Este proceso requiere mucho tiempo.

- Restricciones de espacio

  Cuando se crea un backup de la base de datos, los destinos de registro de archivos se llena, lo que hace que la base de datos no responda hasta que se crea espacio suficiente en el almacenamiento. En SnapManager (3.2 o posterior), se pueden quitar los archivos de registro de archivos del sistema de archivos activo para liberar espacio periódicamente.

Por qué son importantes las copias de seguridad de archivos de registro

Los archivos de registro de archivos son necesarios para avanzar la base de datos después de ejecutar una operación de restauración. Cada transacción en una base de datos Oracle se captura en los archivos archive log (si la base de datos está en el modo archive log). Los administradores de bases de datos pueden restaurar los backups de la base de datos con los archivos de registro de archivos.

Ventajas de las copias de seguridad archivvelog-only

- Proporciona una duración de retención independiente para backups de solo archivado

  Puede tener menos duración de retención para los backups de solo archivado que se requieren para la recuperación.

- Protege los backups de solo archivado basados en políticas de protección de registros de archivos

  Puede seleccionar diferentes políticas de protección para backups de solo archivado en función de sus necesidades.

- Mejora el rendimiento de la base de datos
- Consolida los backups de registros de archivos

  SnapManager consolida los backups de registros de archivos cada vez que se realiza un backup liberando las copias de seguridad duplicadas de los registros de archivo.

Qué son los backups de la base de datos SnapManager

SnapManager permite realizar distintas tareas de backup. Puede asignar clases de retención para especificar cuánto tiempo se puede retener la copia de seguridad; una vez alcanzado ese límite de tiempo, se elimina la copia de seguridad.

- Crear backups en el almacenamiento principal
- Cree backups protegidos en los recursos de almacenamiento secundario
- Compruebe que los backups se han realizado correctamente
- Ver una lista de backups
- Programar las copias de seguridad utilizando la interfaz gráfica de usuario
- Gestión de la cantidad de backups incorporados
- Libere recursos de backup
- Montar y desmontar backups
- Eliminar backups

SnapManager crea backups mediante una de las siguientes clases de retención:

- Cada hora
- Todos los días
- Semanal
- Mensual
- Ilimitada

Protection Manager debe instalarse para utilizar políticas de protección a fin de proteger los backups. Un backup puede tener uno de los siguientes estados de protección: No solicitado, no protegido o protegido.

Si se agregan nuevos archivos de datos a la base de datos, debe crear una copia de seguridad inmediatamente. Además, si restaura una copia de seguridad realizada antes de agregar los nuevos archivos de datos e intenta recuperarse a un punto después de agregar los nuevos archivos de datos, el proceso de recuperación automática podría fallar. Consulte la documentación de Oracle para obtener más información sobre el proceso de recuperación de los archivos de datos agregados después de una copia de seguridad.

Qué son los backups completos y parciales

Puede elegir hacer una copia de seguridad de toda la base de datos o sólo de una parte de ella. Si decide realizar una copia de seguridad de una parte de la base de datos, puede optar por realizar una copia de seguridad de un grupo de tablespaces o archivos de datos. Puede optar por realizar un backup separado de los espacios de tablas y los archivos de datos.

En la siguiente tabla, se enumeran los beneficios y las consecuencias de cada tipo de backup:

Tipo de backup	Ventajas	Desventajas
Lleno	Minimiza el número de copias de Snapshot. Para los backups en línea, cada espacio de tabla está en modo de backup durante todo el tiempo que lleva la operación de backup. SnapManager toma una copia snapshot por cada volumen que utiliza la base de datos, además de una copia snapshot por cada volumen que ocupan los archivos de registro.	Para los backups en línea, cada espacio de tabla está en modo de backup durante todo el tiempo que lleva la operación de backup.
Parcial	Minimiza la cantidad de tiempo que cada espacio de tabla pasa en modo de backup. SnapManager agrupa las copias snapshot que toma por espacio de tabla. Cada espacio de tabla está en modo de backup solo suficientemente tiempo para crear las copias Snapshot. Este método de agrupación de las copias Snapshot minimiza las escrituras de bloque físico en los archivos de registro durante un backup en línea.	El backup puede requerir la creación de copias Snapshot de varios espacios de tablas en el mismo volumen. Este método puede provocar que SnapManager cree varias copias Snapshot de un solo volumen durante la operación de backup.

Nota: aunque puede realizar una copia de seguridad parcial, siempre debe realizar una copia de seguridad completa de toda la base de datos.

Los tipos de backup y la cantidad de copias de Snapshot

El tipo de backup (completo o parcial) afecta al número de copias Snapshot que crea SnapManager. Para un backup completo, SnapManager crea una copia snapshot de cada volumen, mientras que, para un backup parcial, SnapManager crea una copia snapshot de cada archivo de espacio de tabla.

> Data ONTAP limita el número máximo de copias snapshot a 255 por volumen. Solo puede alcanzar este máximo si configura SnapManager para retener un gran número de backups en los que cada backup esté compuesto por numerosas copias de Snapshot.

Para mantener un pool adecuado de backups disponible a la vez que garantiza que no se alcance el límite máximo de copias Snapshot por volumen, debe eliminar backups cuando ya no sean necesarios. Puede configurar la política de retención de SnapManager para eliminar los backups correctos después de alcanzar un umbral específico para una frecuencia de backup específica. Por ejemplo, una vez que SnapManager crea cuatro backups diarios correctos, SnapManager elimina los backups diarios creados en el día anterior.

En las siguientes tablas, se muestra cómo SnapManager crea copias Snapshot según el tipo de backup. El ejemplo de las tablas supone que la base de datos Z incluye dos volúmenes, cada volumen incluye dos

tablespaces (TS1 y TS2) y cada tablespace incluye dos archivos de base de datos (ts1_1.dbf, ts1_2.dbf, ts2_1.dbf y ts2_2.dbf).

En estas tablas, se muestra cómo los dos tipos de backups producen diferentes cantidades de copias Snapshot.

SnapManager crea copias Snapshot a nivel de volumen en lugar del espacio de tabla, lo que reduce normalmente el número de copias Snapshot que debe crear.

Ambos backups también crean copias Snapshot de los archivos de registro.

Volúmenes en la base de datos	Tablespace TS1 (incluye 2 archivos de base de datos)	Tablespace TS2 (incluye 2 archivos de base de datos)	Se crearon copias Snapshot	Número total de copias Snapshot
/Vol/Vola	TS1_1.dbf	TS2_1.dbf	1 por volumen	2

Volúmenes en la base de datos	Tablespace TS1 (incluye 2 archivos de base de datos)	Tablespace TS2 (incluye 2 archivos de base de datos)	Se crearon copias Snapshot	Número total de copias Snapshot
/Vol/Vola	TS1_1.dbf	TS2_1.dbf	2 por archivo	4

Backups completos en línea

Durante un backup online completo, SnapManager realiza un backup de toda la base de datos y crea copias Snapshot en el nivel del volumen (no en el nivel de espacio de tabla).

SnapManager crea dos copias Snapshot para cada backup. Si todos los archivos necesarios para la base de datos se encuentran en un único volumen, las dos copias de Snapshot aparecen en ese volumen.

Cuando se especifica un backup completo, SnapManager realiza las siguientes acciones:

1. Coloca toda la base de datos en el modo de copia de seguridad en línea
2. Crea copias snapshot de todos los volúmenes que contienen archivos de base de datos
3. Saca la base de datos del modo de backup en línea
4. Fuerza un conmutador de registro y, a continuación, archiva los archivos de registro

   Esto también vacía la información de redo en el disco.

5. Genera archivos de control de copia de seguridad
6. Crea una copia snapshot de los archivos de registro y los archivos de control de copia de seguridad

Cuando se realiza un backup completo, SnapManager coloca toda la base de datos en el modo de backup en línea. Un tablespace individual (por ejemplo, /vol/vola/ts1_1.dbf) está en el modo de copia de seguridad en línea más largo que ciertos tablespaces o archivos de datos que se especificaron.

Cuando una base de datos entra en modo de backup, Oracle escribe bloques completos en los registros y no se limita a escribir el delta entre backups. Como las bases de datos trabajan más en modo de backup en línea, elegir un backup completo supone una mayor carga en el host.

Aunque realizar backups completos supone una mayor carga en el host, los backups completos requieren menos copias Snapshot, lo que produce menos requisitos de almacenamiento.

Backups parciales en línea

En lugar de un backup completo, se puede optar por realizar un backup parcial de los espacios de tablas en una base de datos. Mientras SnapManager realiza una copia Snapshot de volúmenes para realizar backups *Full*, SnapManager realiza una copia Snapshot de cada espacio de tabla especificado para *parciales* backups.

Debido a que el nivel de tablespace es el nivel más bajo que Oracle permite en el modo de copia de seguridad, SnapManager procesa las copias de seguridad a nivel de tablespace, incluso si se especifica un archivo de datos en un tablespace.

Con un backup parcial, cada espacio de tabla existe en modo de backup durante un menor tiempo que en un backup completo. Durante un backup en línea, la base de datos siempre está disponible para los usuarios. No obstante, la base de datos debe realizar más trabajo y el host debe ejecutar más operaciones de I/o físicas Asimismo, debido a que se realizan copias Snapshot de cada espacio de tabla especificado o cada espacio de tabla que contiene un archivo de datos especificado en lugar de todo el volumen, SnapManager realiza más copias Snapshot.

SnapManager realiza copias Snapshot de espacios de tablas o archivos de datos específicos. El algoritmo de copia de seguridad parcial es un bucle que SnapManager repite hasta que ha tomado una copia snapshot de cada tablespace o archivo de datos especificado.

> Aunque se puede realizar un backup parcial, se recomienda realizar siempre un backup completo de toda la base de datos.

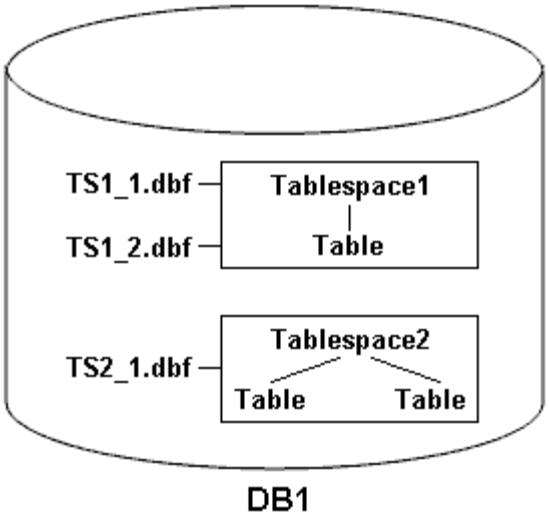
Durante un backup parcial, SnapManager realiza las siguientes acciones:

1. Coloca el tablespace que contiene los archivos de datos en modo de copia de seguridad.
2. Toma una copia Snapshot de todos los volúmenes utilizados por el espacio de tablas.
3. Quita el tablespace del modo de copia de seguridad.
4. Continúa este proceso, hasta que ha tomado una copia snapshot de todos los espacios de tablas o archivos.
5. Fuerza un conmutador de registro y, a continuación, archiva los archivos de registro.
6. Genera archivos de control de copia de seguridad.
7. Toma una copia snapshot de los archivos de registro y los archivos de control de copia de seguridad.

Ejemplos de operaciones de backup, restauración y recuperación

Puede encontrar información sobre algunos de los escenarios de backup, restauración y recuperación que puede usar para lograr sus objetivos de protección de datos.

En la siguiente ilustración se muestra el contenido del tablespace:



En la ilustración, Tabespace1 tiene una tabla y dos archivos de base de datos asociados. Tabespace2 tiene dos tablas y un archivo de base de datos asociado.

En las siguientes tablas se describen algunos escenarios de backup, restauración y recuperación completos y parciales:

Ejemplos de operaciones de backup, restauración y recuperación completas

Backup completo	Restaurar	Recuperación
SnapManager realiza un backup del todo en la base de datos DB1, incluidos los archivos de datos, los registros de archivo y los ficheros de control.	La restauración completa con archivos de control SnapManager restaura todos los archivos de datos, espacios de tablas y archivos de control en el backup.	Puede especificar una de las opciones siguientes: • SCN: Introduzca un SCN, como 384641. • Fecha/hora: Introduzca una fecha y hora de la copia de seguridad, como 2005-11-25:19:06:22. • La última transacción realizada a la base de datos.
Restauración completa sin archivos de control SnapManager restaura todos los espacios de tablas y archivos de datos, sin los archivos de control.	Cuando se restauran los archivos de datos o los espacios de tablas con archivos de control, se especifica una de las siguientes opciones: • Espacios de tabla • Archivos de datos	SnapManager recupera los datos a la última transacción realizada a la base de datos.

Ejemplos de operaciones de backup, restauración y recuperación parciales

Copia de seguridad parcial	Restaurar	Recuperación
Es posible elegir una de las siguientes opciones: • Espacios de tabla Puede especificar Tablespaca1 y Tabespaca2 o sólo uno de ellos. • Archivos de datos Puede especificar los tres archivos de base de datos (TS1_1.dbf, TS1_2.dbf y TS2_1.dbf), dos archivos o un archivo. Independientemente de la opción que seleccione, el backup incluirá todos los archivos de control. Los archivos de registro de archivos se incluyen en el backup parcial si el perfil no está habilitado para crear los backups de los registros de archivos por separado.	La restauración completa de SnapManager restaura todos los archivos de datos, los espacios de tablas y los archivos de control especificados en el backup parcial.	SnapManager recupera los datos a la última transacción realizada a la instancia de la base de datos.

Copia de seguridad parcial	Restaurar	Recuperación
Restaure los archivos de datos o los espacios de tablas con los archivos de control SnapManager restaura uno de los siguientes elementos: • Todos los archivos de datos especificados • Todos los espacios de tablas especificados	Restaure los archivos de datos o los espacios de tablas sin los archivos de control SnapManager restaura uno de los siguientes elementos: • Espacios de tabla Especifique cualquiera de los espacios de tablas. SnapManager restaura solo los espacios de tablas especificados. Si la copia de seguridad contiene tablespace1, SnapManager sólo restaura ese tablespace. • Archivos de datos Especifique cualquiera de los archivos de la base de datos. SnapManager solo restaura los archivos de datos especificados. Si la copia de seguridad contiene archivos de base de datos (TS1_1.dbf y TS1_2.dbf), SnapManager sólo restaura esos archivos.	Únicamente restaure los archivos de control

Acerca del manejo de archivos de registro de archivo y archivos de control

SnapManager incluye los archivos de control y, opcionalmente, incluye los archivos de registro de archivo en cada backup. Los archivos de registro de archivo se usan para operaciones de recuperación.

La base de datos utiliza archivos de control para identificar nombres, ubicaciones y tamaños de los archivos de base de datos. SnapManager incluye los archivos de control en cada backup porque los archivos de control se utilizan en el proceso de restauración.

Se hace un seguimiento de los cambios en una base de datos mediante los redo logs en línea, que finalmente se archivan y se conocen como redo logs archivados (o archive logs). SnapManager (3.2 o posterior) permite realizar backups de los archivos de datos y los archivos de registro de archivos de forma independiente con diferentes retentions y frecuencias. SnapManager puede realizar backups únicamente de los registros de archivo o los backups combinados de archivos de datos y registros de archivos. SnapManager ofrece una gestión automatizada completa de los registros de archivos, y no requiere intervención manual para la recuperación de bases de datos. Además, permite la eliminación de registros de archivos de uno o más destinos de registros de archivos después de realizar el backup.

Para ver qué tablespaces y archivos de datos se incluyen en una copia de seguridad, utilice el comando backup show o la ventana Backup Properties.

La siguiente tabla muestra cómo SnapManager gestiona los archivos de control y de registro de archivo durante cada operación:

[options="header"]d

Tipo de operación	Archivos de control	Archivos de registro de archivo
Backup	Incluidas con cada backup	Se puede incluir con cada backup
Restaurar	Se pueden restaurar por separado o junto con los espacios de tablas o los ficheros de datos	Se puede usar para el proceso de recuperación

Qué es la programación de backups de base de datos

Puede programar, actualizar y supervisar las copias de seguridad de las bases de datos mediante la ficha Programación de la interfaz gráfica de usuario.

La siguiente tabla aborda algunas preguntas frecuentes sobre la programación:

Pregunta	**Responda**
¿Qué ocurre con los backups programados al reiniciarse el servidor de SnapManager?	Cuando se reinicia el servidor SnapManager, éste reinicia automáticamente todas las programaciones. Sin embargo, SnapManager no realiza seguimiento de ninguna incidencia perdida.

Pregunta	Responda
¿Qué sucede cuando se programan dos backups en dos bases de datos a la vez?	SnapManager inicia las operaciones de backup de uno en uno y luego permite que los backups se ejecuten en paralelo. Por ejemplo, si un administrador de bases de datos crea seis programaciones de backup diarias para seis perfiles de base de datos diferentes a las 00:00, los seis backups se ejecutan en paralelo. Si se programan varios backups en un único perfil de base de datos en un breve periodo de tiempo, el servidor SnapManager ejecutará solo la operación de backup con la duración de retención más larga. Antes de iniciar una operación de backup, SnapManager primero determina lo siguiente: • En los últimos 30 minutos, ¿ha creado otra programación correctamente un backup, con mayor retención, para el mismo perfil? • En los próximos 30 minutos, ¿intentará otra programación crear un backup, con mayor retención, para el mismo perfil? Si la respuesta a cualquiera de las dos preguntas es sí, SnapManager omite el backup. Por ejemplo, un administrador de bases de datos puede crear una programación diaria, semanal y mensual para un perfil de base de datos, y se prevé que todos los backups se realicen a las 1:00 a.m. En ese día del mes en el que se programan tres backups a la vez a las 1:00, SnapManager únicamente ejecutará la operación de backup en función de la programación mensual. La ventana de tiempo de 30 minutos se puede cambiar en un archivo de propiedades de SnapManager.
¿Con qué usuario se ejecuta la operación de backup?	La operación se ejecuta bajo el usuario que creó la programación. Sin embargo, es posible cambiarlo por su propio ID de usuario, si cuenta con credenciales válidas tanto para el perfil de base de datos como para el host. Por ejemplo, al iniciar las propiedades de copia de seguridad programada para la programación de copia de seguridad creada por Avida Davis, Stella Morrow puede seleccionar su ID de usuario en realizar esta operación como usuario para ejecutar la copia de seguridad programada.

Pregunta	Responda
¿Cómo interactúa el programador de SnapManager con el programador del sistema operativo nativo?	En el servidor SnapManager, no se pueden ver los backups programados a través del planificador nativo del sistema operativo. Por ejemplo, después de crear una copia de seguridad programada, no se ve ninguna entrada adicional en cron.

Pregunta	Responda
¿Qué sucede si los relojes de la interfaz gráfica de usuario y el servidor no están sincronizados?	Los relojes del cliente y del servidor no están sincronizados. Por lo tanto, puede programar una copia de seguridad en la que la hora de inicio esté en el futuro en el cliente pero en el pasado en el servidor. Para realizar backups periódicos, el servidor sigue cumpliendo la solicitud. Por ejemplo, si el servidor recibe una solicitud para realizar copias de seguridad cada hora a partir del 01/30/08 a las 3:00 p.m. pero la hora actual es a las 3:30 p.m. ese día, el servidor realiza su primer backup a las 4:00 p.m. y continúa realizando backups cada hora. Sin embargo, durante los backups que solo se realizan una vez, el servidor gestiona la solicitud de la siguiente forma: • Si la hora de inicio está dentro de los últimos cinco minutos de la hora del servidor actual, SnapManager inicia de inmediato el backup. • Si la hora de inicio es superior a cinco minutos, SnapManager no inicia el backup. Por ejemplo, piense en el siguiente escenario: • El reloj del host de la interfaz gráfica está a tres minutos de distancia del tiempo real. • La hora actual en el cliente es 8:58 a.m. • Se programa un backup puntual a las 9:00 • Se programa otro backup que se realice una vez a las 8:30 Cuando el servidor recibe la primera solicitud, la hora en el servidor es 9:01 a.m. Aunque la hora de inicio del backup es anterior, SnapManager realiza el backup de forma inmediata. Cuando el servidor recibe la segunda solicitud, la hora de inicio del backup ha pasado más de cinco minutos. Recibirá un mensaje indicando que la solicitud de programa ha fallado porque la hora de inicio ha pasado. Puede cambiar el tiempo de cinco minutos en un archivo de propiedades de SnapManager.
¿Qué ocurre en los backups programados para un perfil cuando se elimina el perfil?	Cuando se elimina un perfil de base de datos, el servidor SnapManager elimina los backups programados definidos para ese perfil.

Pregunta	Responda

¿Cómo se comportan los backups programados durante el horario de verano o cuando se cambia la hora del servidor SnapManager?	Las programaciones de backups de SnapManager se ven afectadas por el horario de verano o al cambiar la hora del servidor SnapManager.
	
	Tenga en cuenta las siguientes implicaciones cuando cambie el tiempo del servidor SnapManager:
	
	• Después de activar la programación de copia de seguridad, si la hora del servidor SnapManager se reduce, la programación de copia de seguridad no se activa de nuevo.
	• Si la hora de verano comienza antes de la hora de inicio programada, las programaciones de backup se activan automáticamente.
	• Por ejemplo, si se encuentra en los Estados Unidos y se programan los backups cada hora a las 4:00 esto se debe producir cada 4 horas, se realizará un backup a las 4:00, 8:00, 12:00, 4:00, 8:00, Y medianoche los días antes y después de los ajustes de horario de verano en marzo y noviembre.
	• Tenga en cuenta lo siguiente si las copias de seguridad están programadas para las 2:30 a.m. todas las noches:
	  ◦ Cuando los relojes se atrasan una hora, ya que el backup se activa, el backup no se activa de nuevo.
	  ◦ Cuando los relojes se adelantan una hora, el backup se activa inmediatamente. Si se encuentra en los Estados Unidos y desea evitar este problema, debe programar las copias de seguridad para que comiencen fuera de las 2:00 a.m. a las 3:00 horas intervalo.

Creación de backups de la base de datos

Puede crear backups de bases de datos completas o de partes de bases de datos, incluidos espacios de tabla, archivos de datos o archivos de control.

SnapManager proporciona funcionalidades de copia de Snapshot para bases de datos en muchas pilas de almacenamiento del lado del host, incluidas NFS, ASM, Veritas, etc.

> Para configuraciones de Real Application Clusters (RAC), SnapManager realiza el backup en el lado del host en el perfil.

Los administradores pueden opcionalmente registrar backups con Oracle RMAN, lo que facilita el uso de RMAN para restaurar y recuperar la base de datos con granularidades más finas como bloques.

Al definir el perfil, puede personalizar los nombres de las copias Snapshot creadas por backups de ese perfil. Por ejemplo, puede insertar una cadena de prefijo del NÚMERO DE SALTOS para indicar backups de operaciones altas.

Además de definir nombres únicos para las copias de Snapshot creadas por backups, también puede crear etiquetas únicas para los propios backups. Cuando se crea un backup, se recomienda proporcionar un nombre para el backup de forma que se cuente con un método sencillo para identificarlo con el parámetro -label. Este nombre debe ser único para todos los backups creados dentro de un perfil determinado. El nombre puede contener letras, números, guiones bajos (_) y guiones (-). No puede comenzar con un guión. Las etiquetas distinguen mayúsculas de minúsculas. Puede incluir información como variables de entorno del sistema operativo, fecha del sistema y tipo de backup.

Si no proporciona una etiqueta, SnapManager crea un nombre de etiqueta predeterminado en la forma scope_mode_datestring, donde el ámbito está completo o parcial y el modo está sin conexión, en línea o automático (la letra c para frío, h para caliente o a para automático).

Desde SnapManager 3.4, puede proporcionar su propia etiqueta de backup reemplazando la etiqueta de backup predeterminada que creó SnapManager. Debe configurar el valor del parámetro override.default.backup.pattern en TRUE y especificar la nueva etiqueta de backup en el parámetro new.default.backup.pattern. El patrón de etiqueta de backup puede contener palabras clave como el nombre de la base de datos, el nombre del perfil, el ámbito, el modo y el nombre de host, que deben separarse con el guión bajo. Por ejemplo, new.default.backup.pattern=dbname_profile_hostname_scope_mode.

La Marca de hora se incluirá automáticamente al final de la etiqueta generada.

Al introducir un comentario, puede incluir espacios y caracteres especiales. Por el contrario, cuando introduzca una etiqueta, no incluya espacios ni caracteres especiales.

Para cada backup, SnapManager genera automáticamente un GUID, que es una cadena HEXADECIMAL de 32 caracteres. Para determinar el GUID, debe ejecutar el comando backup list con la opción -verbose.

Es posible crear un backup completo de una base de datos mientras está en línea o sin conexión. Para permitir que SnapManager gestione el backup de una base de datos independientemente de si está en línea o sin conexión, debe utilizar la opción -auto.

Al crear un backup, si se habilitó la eliminación y se habilitó la notificación de resumen en el perfil, se activan dos correos electrónicos independientes. Un correo electrónico es para la operación de backup y el otro para la eliminación. Es posible correlacionar estos correos electrónicos comparando el nombre de la copia de seguridad y el ID de copia de seguridad incluidos en estos correos electrónicos.

Es posible crear un backup en frío cuando la base de datos está en estado de apagado. Si la base de datos está en estado montado, cambie a estado de apagado y realice el backup sin conexión (backup en frío).

SnapManager (3.2 o posterior) permite realizar un backup de los archivos de registro de archivos independientemente de los archivos de datos, lo que permite gestionar los archivos de registro de archivos de forma eficiente.

Para crear los backups de registros de archivos por separado, debe crear un nuevo perfil o actualizar el perfil existente para separar los backups de los registros de archivos con la opción -separate-archivvelog-backups. Con el perfil, es posible realizar las siguientes operaciones de SnapManager:

- Cree un backup de registro de archivos.
- Eliminar un backup de registro de archivos.

- Montar un backup de registro de archivos.
- Liberar un backup de registro de archivo.

Las opciones de copia de seguridad varían en función de la configuración del perfil:

- Si se utiliza un perfil que no está separado para realizar backups de registros de archivos de forma independiente, se puede hacer lo siguiente:
  - Cree un backup completo.
  - Crear un backup parcial.
  - Especifique los destinos de registros de archivos que se incluirán en el backup para los archivos de registro de archivos.
  - Especifique los destinos de registro de archivos que se excluirán de la copia de seguridad.
  - Especifique las opciones de eliminación para eliminar los archivos de registro de archivos de los destinos de registro de archivos.
- El uso de un perfil separado para tomar backups de registros de archivos permite hacer lo siguiente:
  - Cree una copia de seguridad sólo de archivos de datos.
  - Cree un backup solo de archivado.
  - Durante la creación de un backup solo de archivos de datos, incluya el backup de registro de archivos junto con el backup en línea de solo los archivos de datos para el clonado.

    Si ha incluido copias de seguridad de registros de archivos junto con archivos de datos en la página **Configuración de perfiles** del asistente **creación de perfiles** de la interfaz gráfica de usuario de SnapManager, Y si no ha seleccionado la opción **Archivelogs** en el asistente **creación de copia de seguridad**, SnapManager siempre crea la copia de seguridad del registro de archivos junto con los archivos de datos para todas las copias de seguridad en línea.

    En tal situación, en la CLI de SnapManager, puede tener en cuenta todos los destinos de los registros de archivos para el backup, excepto los destinos de exclusión especificados en el archivo de configuración SnapManager. Pero no puede eliminar estos archivos de registro de archivos. Sin embargo, puede seguir utilizando la opción -archivovelogs para especificar el destino del archivo de registro de archivos y hacer un uso de los archivos de registro de archivos desde la interfaz de línea de comandos de SnapManager.

    Si crea el backup con la opción -auto y especifica la opción --archivelogs, SnapManager crea un backup en línea o sin conexión según el estado actual del backup.

    - SnapManager crea un backup sin conexión cuando la base de datos está sin conexión y no incluye los archivos de registro de archivos en el backup.
    - SnapManager crea un backup en línea incluidos los archivos de registro de archivos cuando la base de datos está en línea.
  - Mientras se crea el backup de solo archivado:
    - Especifique el destino de registro de archivos que se realizará el backup junto con el backup solo de archivmogs
    - Especifique los destinos de registro de archivos que se excluirán del backup solo de registros de archivo
    - Especifique las opciones de eliminación para eliminar los archivos de registro de archivos de los destinos de registro de archivos

- **Escenarios no admitidos**
  - No puede crear el backup solo de archivado junto con un backup de solo archivos de datos sin conexión.
  - No se pueden reducir los archivos de registro de archivos cuando no se realiza el backup de los archivos de registro de archivos.
  - No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos.

    Si especifica la ubicación del registro de archivos en el área de recuperación flash, debe asegurarse de especificar también la ubicación del registro de archivos en el parámetro archive_log_dest.

Al especificar la etiqueta para la copia de seguridad de archivos de datos en línea con la copia de seguridad de archivos de archivo incluida, se aplica la etiqueta para la copia de seguridad de archivos de datos, y la copia de seguridad del registro de archivo se adjuntará con el sufijo (_logs). Este sufijo puede configurarse cambiando el parámetro suffix.backup.label.with.logs en el archivo de configuración de SnapManager.

Por ejemplo, puede especificar el valor como suffix.backup.label.with.logs=Arc para que el valor predeterminado _logs cambie a _Arc.

Si no se especificaron destinos de registro de archivos para su inclusión en el backup, SnapManager incluye todos los destinos de registro de archivos configurados en la base de datos.

Si falta algún archivo de registro de archivo en alguno de los destinos, SnapManager omite todos estos archivos de registro de archivos creados antes de los archivos de registro de archivos que faltan aunque estos archivos estén disponibles en otro destino de registro de archivos.

Al crear backups de registros de archivos, es necesario especificar los destinos de archivos de registro de archivos que se incluirán en el backup. Además, puede configurar el parámetro Configuration para incluir los archivos de registro de archivos siempre más allá de los archivos faltantes en el backup.

> De forma predeterminada, este parámetro de configuración se establece en TRUE para incluir todos los archivos de registro de archivos, más allá de los archivos que faltan. Si utiliza sus propios scripts de eliminación de registros de archivos o eliminación manual de archivos de registro de archivos de los destinos de registro de archivos, puede deshabilitar este parámetro, para que SnapManager pueda omitir los archivos de registro de archivos y continuar con el backup.

SnapManager no admite las siguientes operaciones SnapManager para backups de registros de archivos:

- Clone el backup de registros de archivos
- Restaurar el backup de registros de archivos
- Verificar el backup de registros de archivos

SnapManager también admite la copia de seguridad de los archivos de registro de archivos desde los destinos de área de recuperación flash.

1. Introduzca el siguiente comando: smo backup create -profile_name {[-full {-online | -offline | -auto} [-retain {-hora | -diario | -semanal | -mensual | -ilimitado}] [-verify] | [-data [-filesfiles [ficheros] | [-tablespaces [-commentation]]] [-datalabellabel] | -retain] | -compointing] [-snapvaultlabelSnapVault_label][-Protect | -noProtect | -protectnoow] [-backup-destinpath1 [,[path2]] [-exclude-destinpath1 [,path2]] [-pruns {-all | -untilSCtilSCN | -until-date yyyy-MM-dunch-toune | -days] [-prunch-prunx] -dunch-prunx]

Si desea…	Realice lo siguiente…
Cree una copia de seguridad en el almacenamiento secundario mediante la directiva de protección de SnapManager_CDOT_Vault_	Especifique la etiqueta -snapvault. Debe proporcionar la etiqueta de SnapMirror que haya especificado en las reglas de la política de SnapMirror al configurar la relación de SnapVault como valor.
Especifique si desea realizar una copia de seguridad de una base de datos en línea o sin conexión, en lugar de permitir que SnapManager controle si está en línea o sin conexión	Specify -offline para realizar un backup de la base de datos sin conexión. Specify -online para realizar un backup de la base de datos en línea. + Si utiliza estas opciones, no puede utilizar la opción -auto.
Especifique si desea que SnapManager gestione la copia de seguridad de una base de datos independientemente de si está en línea o sin conexión	Especifique la opción -auto. Si utiliza esta opción, no podrá utilizar la opción --offline o -online.

Especifique si desea realizar una copia de seguridad parcial de archivos específicos	`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.`
	`+ ejemplo para crear una copia de seguridad parcial del archivo de datos en UNIX`
	
	+
	
	`smo backup create -profile nosep -data -files /user/user.dbf -online -label partial_datafile_backup -verbose`

Si desea…	Realice lo siguiente…

Especifique si desea realizar una copia de seguridad parcial de tablespaces específicos	`Specify the -data-tablespaces option and then list the tablespaces, separated by commas. For example, use ts1, ts2, and ts3 after the option.`
	`+ SnapManager permite realizar backup de espacios de tablas de solo lectura. Al crear el backup, SnapManager cambia los espacios de tabla de solo lectura a lectura y escritura. Después de crear el backup, los espacios de tabla se modifican a modo de solo lectura.`
	
	+ ejemplo para crear una copia de seguridad de tablespace parcial
	
	+
	
	`smo backup create -profile nosep -data -tablespaces tb2 -online -label partial_tablespace_bkup -verbose`

Especifique si desea crear una etiqueta única para cada copia de seguridad en el siguiente formato: 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`

Si desea…	Realice lo siguiente…

Especifique si desea crear una copia de seguridad de los archivos de registro de archivos por separado de los archivos de datos	`Specify the following options and variables:`
	`** -archivvelogs crea una copia de seguridad de los archivos de registro de archivo.`
	`** -backup-dest especifica los destinos de archivos de registro de archivos que se incluirán en el backup.`
	`** -exclude-dest especifica los destinos de registro de archivos que se van a excluir.`
	`** -label especifica la etiqueta para el backup del archivo de registro de archivos.`
	`** -protect permite proteger los backups de registros de archivos.`
	`*Nota:* debe proporcionar la opción -backup-dest o la opción -exclude-dest.`
	
	+ Si se proporcionan ambas opciones junto con la copia de seguridad, se muestra un mensaje de error que ha especificado una opción de copia de seguridad no válida. Especifique una de las opciones: -Backup-dest o exclude-dest.
	
	+ Ejemplo de creación de backups de archivos de registro de archivos por separado en UNIX
	
	+
	
	`smo backup create -profile nosep -archivelogs -backup-dest /mnt/archive_dest_2/ -label archivelog_bkup -verbose`

Si desea…	Realice lo siguiente…

Especifique si desea crear una copia de seguridad de archivos de datos y archivos de registro de archivos juntos	`Specify the following options and variables:`
	`** -data option para especificar los archivos de datos.`
	`** -archivelogs opción para especificar los archivos de registro de archivos. Ejemplo para realizar backups de archivos de datos y archivos de registro de archivos juntos en UNIX`
	+
	`smo backup create -profile nosep -data -online -archivelogs -backup-dest  mnt/archive_dest_2 -label data_arch_backup -verbose`

Si desea…	Realice lo siguiente…

Especifique si desea eliminar los archivos de registro de archivos mientras crea una copia de seguridad	`Specify the following options and variables:`
	`** -prunelogs especifica que se eliminen los archivos de registro de archivos de los destinos de registro de archivos.`
	
	+ *** -all especifica que se eliminen todos los archivos de registro de archivos de los destinos de registro de archivos.** * -Until-scnuntil-scn especifica que se eliminen los archivos de registro de archivos hasta un SCN especificado. *** -Until -dateyyyy-MM-dd:HH:mm:ss especifica que se eliminen los archivos de registro de archivos hasta el período de tiempo especificado.** * la opción -before especifica la eliminación de los archivos de registro de archivos antes del período de tiempo especificado (días, meses, semanas, horas). ***** -prune-destprune_dest1,[prune_dest2 especifica que se eliminen los archivos de registro de archivo de los destinos de registro de archivo mientras se crea la copia de seguridad. **Nota:** no puede pinar los archivos de registro de archivos cuando el área de recuperación de Flash (FRA) está activada para archivos de registro de archivos.
	
	+ Ejemplo de eliminación de todos los archivos de registro de archivos mientras se crea una copia de seguridad en 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`

Especifique si desea añadir un comentario sobre la copia de seguridad	Especifique -comment seguido de la cadena de descripción.

Si desea…	Realice lo siguiente…
Especifique si desea forzar la base de datos al estado que ha especificado para realizar la copia de seguridad, independientemente del estado en el que se encuentre	Especifique la opción -force.
Especifique si desea verificar la copia de seguridad al mismo tiempo que la crea	Especifique la opción -Verify.
Especifique si desea recopilar los archivos de volcado después de la operación de copia de seguridad de la base de datos	Especifique la opción -dump al final del comando de creación de backup.

Ejemplo

```
smo backup create -profile targetdb1_prof1 -full -online -force  -verify
```

Información relacionada

Nomenclatura de copias Snapshot

Crear scripts de tareas previas, tareas posteriores y directivas

Creación de scripts de tareas

Almacenamiento de los scripts de tareas

El comando smo backup create

Protección de backups de bases de datos en almacenamiento secundario o terciario

Eliminar archivos de registro de archivos

Puede reducir los archivos de registro de archivos desde las ubicaciones del registro de archivos mientras crea una copia de seguridad.

- La operación de backup actual debe realizar un backup de los archivos de registro de archivos.

  Si se especifica la eliminación junto con otros backups que no contienen archivos de registro de archivos, no se reducen los archivos de registro de archivos.

- La base de datos debe estar en el estado montado.

  Si la base de datos no está en estado montado, introduzca la opción -force junto con el comando de backup.

Al realizar una operación de backup, se puede especificar lo siguiente:

- Ámbito de la eliminación:

- Elimine todos los archivos de registro de archivos.
- Elimine los archivos de registro de archivos hasta que el SCN especificado.
- Elimine los archivos de registro de archivos hasta la hora especificada.
- Elimine los archivos de registro de archivos antes del período de tiempo especificado.

- Destino desde el que se deben quitar los archivos de registro de archivos.

> Aunque se produzca un error al eliminar el archivo de registro de archivos en un destino, SnapManager continúa depurando los archivos de registro de archivos de los otros destinos.

Antes de eliminar los archivos de registro de archivos, SnapManager verifica lo siguiente:

- Se realiza un backup de los archivos de registro de archivo al menos una vez.
- Los archivos de registro de archivo se envían a la base de datos Oracle Dataguard Standby, si los hubiera.
- El proceso de captura de Oracle Streams captura los archivos de registro de archivo, si los hay.

Si se realiza un backup de los archivos de registro de archivos, se envían al estado de espera y se capturan mediante el proceso de captura, SnapManager elimina todos los archivos de registro de archivos en una sola ejecución. Sin embargo, si hay archivos de registro de archivos que no se incluyen en un backup, que no se envían a en espera o que no están capturados por el proceso de captura, SnapManager elimina los archivos de registro de archivos uno por uno. La eliminación de archivos de registros de archivos en una sola ejecución es más rápida que la eliminación de registros de archivos uno por uno.

SnapManager también puede agrupar los archivos de registro de archivos y eliminarlos por lotes. Cada lote tendrá un máximo de 998 archivos. Este valor se puede configurar por debajo de 998 utilizando el parámetro de configuración Maximum.archivvelog.files.torune.atATime en el archivo smo.config.

SnapManager utiliza los comandos de Oracle Recovery Manager (RMAN) para eliminar los archivos de registro de archivo. Sin embargo, SnapManager no se integra con las políticas de retención y de eliminación de RMAN.

> Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.

SnapManager no admite la eliminación de archivos de registro de archivos en las siguientes situaciones:

- Los archivos de registro de archivo se encuentran en el área de recuperación de flash.
- Los archivos de registro de archivo se encuentran en la base de datos en espera.
- SnapManager y RMAN gestionan los archivos de registro de archivo.
  a. Introduzca el siguiente comando: smo backup create -profile_name {[-full {-online | -offline | -auto} [-retenga {-hora | [-diaria | -semanal | -mensual | -unlimited}] [-verify] | [-data [-lablothora archivos [archivos] | [-tablespaces [-commentation]] [-compointing] | -retain] [-Protect | -noProtect | -protectnoow] [-backup-destinpath1 [,[path2]]] [-exclude-destinpath1 [,path2]] [-pruns {-all | -untilSCNuntilSCN | -unce -unce-desteyyyy-MM-espec:HH:mm:ss | -dunch-prune | -pays] -pays] -pays]

Si desea…	Realice lo siguiente…
Prune archive log files	Especifique las siguientes opciones: • -prunelogs especifica la eliminación de los archivos de registro de archivos mientras se crea un backup. ◦ -all especifica la eliminación de todos los archivos de registro de archivos. ◦ -UntilSCN especifica la eliminación de los archivos de registro de archivos hasta el SCN especificado. ◦ -until-date especifica la eliminación de los registros de archivo incluyendo la fecha y hora especificadas. ◦ -antes de {-meses
-días	-semanas
-hours} especifica la eliminación de los archivos de registro de archivos antes del periodo de tiempo especificado.	• Incluir el destino desde donde se van a quitar los archivos de registro *

Consolidación de backups de registros de archivos

SnapManager consolida los backups de solo archivado cada vez que realiza un backup liberando únicamente los backups duplicados de archivvelog. La consolidación está habilitada de forma predeterminada.

SnapManager identifica los backups solo de archivado que tienen archivos de registro de archivos en otros backups y los libera para mantener la cantidad mínima de backups de solo archivado con archivos de registro únicos.

Si la consolidación libera los backups de solo archivado, estos backups se eliminan según la duración de la retención del registro de archivos.

Cuando la base de datos se encuentra en el estado shutdown o nomount durante la consolidación del registro de archivo, SnapManager cambia la base de datos al estado Mount.

Si se produce un error en la copia de seguridad o la eliminación de archivos de registro de archivos, no se realizará la consolidación. La consolidación de backups de solo archivovelog se sigue solo después de backups correctos y de operaciones de eliminación correctas.

1. Para permitir la consolidación de los backups de solo archivado, modifique la consolidación de los parámetros de configuración y establezca el valor como TRUE en el archivo de configuración SnapManager (smo.config).

   Una vez configurado el parámetro, se consolidan los backups de solo archivado.

   Si el backup de solo archivado creado recientemente contiene los mismos archivos de registro de archivos en cualquiera de los backups de solo archivado anteriores, se liberan los backups de solo registros de archivos anteriores.

SnapManager no consolida el backup de registros de archivos realizado junto con el backup de archivos de datos. SnapManager consolida el backup de solo archivado.

SnapManager consolida los backups de registros de archivos, incluso cuando el usuario elimina manualmente los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados y pueden incluirse el backup.

2. Para deshabilitar la consolidación de los backups de registros de archivo, modifique la consolidación de los parámetros de configuración y establezca el valor como FALSE en el archivo de configuración de SnapManager (smo.config).

Programar la eliminación del archivo de registro de archivos

Cuando se crea un backup, es posible programar la eliminación de los archivos de registro de archivos para que se produzca en un momento determinado.

SnapManager permite reducir periódicamente los archivos de registro de archivos desde el sistema de archivos activo.

1. Introduzca el siguiente comando: `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]`

Si desea…	Realice lo siguiente…
Programar la eliminación de archivos de registro de archivos	Especifique las siguientes opciones: • -prunelogs para programar la eliminación de los archivos de registro de archivo • -prune-dest para depurar archivos de registro de archivos desde los destinos de registro de archivos
Incluya un nombre para el horario	Especifique la opción -schedule-name.

Si desea…	Realice lo siguiente…
Programar la eliminación de archivos de registro de archivos en un intervalo de tiempo específico	Especifique la opción INTERVAL e indique si los archivos log de archivo deben recordarse en función de las siguientes clases de intervalo: • -cada hora • - diariamente • -semanal • -mensual • -untimeonly
Agregar un comentario sobre la operación de horario	Especifique la opción -schedule-comment seguida de la cadena de descripción.
Especifique la hora de inicio de la operación de programación	Especifique la opción -start-time en el formato yyyy-mm-dd hh:mm.

Protección de backups de registros de archivos

Al crear perfiles, puede habilitar la protección para los backups del registro de archivos según la política de protección de los registros de archivos.

1. Introduzca el siguiente comando: `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]`

Si…	Realice lo siguiente…
Desea realizar una copia de seguridad de las copias de seguridad de archive log por separado y proteger los archivos archive log	Especifique las siguientes opciones: • -separar-archivvelog-backups permite separar los archivos log de los archivos de datos. • -protect asigna una política de protección independiente para los backups de los registros de archivos de registros de archivos. • -protection-policy asigna la política de protección para los backups de registros de archivos.

Qué es AutoSupport

La función AutoSupport permite que el servidor SnapManager envíe mensajes de AutoSupport al sistema de almacenamiento una vez completada la operación de backup.

SnapManager envía mensajes de AutoSupport solo para las operaciones de backup correctas.

Puede habilitar o deshabilitar AutoSupport asignando los siguientes valores al parámetro de configuración auto_support.on en el archivo de configuración de smo.config:

- TRUE - habilita AutoSupport
- FALSE - deshabilita AutoSupport

De manera predeterminada, AutoSupport se habilita en SnapManager.

Información relacionada

Añadir sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager

Habilitar AutoSupport en SnapManager

Deshabilitar AutoSupport en SnapManager

Añadir sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager

Debe añadir los sistemas de almacenamiento operativos en Clustered Data ONTAP al host del servidor de SnapManager para habilitar AutoSupport. En SnapManager 3.3 y versiones anteriores, AutoSupport solo era compatible con sistemas de almacenamiento que funcionaban en 7-Mode.

1. Añada sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager.

Si…	Después, ejecute el siguiente comando…
La máquina virtual de almacenamiento de administración (SVM, antes denominada Vserver) está funcionando en Clustered Data ONTAP	SnapDrive config set -cserver user_namestorage_name
SVM opera en Clustered Data ONTAP	SnapDrive config set -vserver usuario_namestorage_name

Habilitar AutoSupport en SnapManager

Debe habilitar AutoSupport, de modo que los sistemas de almacenamiento reciban mensajes del servidor SnapManager para cada operación de backup realizada correctamente.

AutoSupport se puede habilitar de dos formas:

- De forma predeterminada, la nueva instalación de SnapManager no contiene el parámetro auto_support.on en el archivo de configuración smo.config. Esto implica que AutoSupport está habilitado.
- Puede configurar manualmente el parámetro auto_support.on.
  a. Detenga el servidor SnapManager.
  b. En el archivo de configuración smo.config, establezca el valor del parámetro auto_support.on en TRUE.

     auto_support.on=TRUE

  c. Reinicie el servidor SnapManager.

Deshabilitar AutoSupport en SnapManager

Debe deshabilitar AutoSupport si no desea que el sistema de almacenamiento reciba mensajes del servidor SnapManager para cada operación de backup exitosa.

De manera predeterminada, AutoSupport se habilita si el archivo de configuración no contiene el parámetro auto_support.on. En este escenario, debe agregar el parámetro auto_support.on en el archivo de configuración y establecer el valor EN FALSE.

1. Detenga el servidor SnapManager.
2. En el archivo de configuración smo.config, establezca el valor del parámetro auto_support.on en FALSE.

   auto_support.on=FALSE

3. Reinicie el servidor SnapManager.

Verificación de los backups de las bases de datos

Es posible utilizar el comando backup verify para verificar que los bloques del backup de la base de datos no están dañados. La operación Verify invoca la utilidad Oracle Database Verify para cada archivo de datos de la copia de seguridad.

SnapManager permite realizar la operación de verificación cuando lo desee, tanto para usted como para los usuarios del sistema. Es posible realizar la verificación inmediatamente después de crear el backup. Debe especificar el perfil que contiene el backup y la etiqueta o el ID del backup creado.

> Es posible especificar -dump para recoger los archivos de volcado después de la operación de verificación de backup.

1. Introduzca el siguiente comando: `smo backup verify -profile profile_name [-label label | -idid] [-force] [ -dump] [-quiet | -verbose]`

Información relacionada

El comando smo backup verify

Cambiar la política de retención de backups

Puede cambiar las propiedades de un backup para que sea elegible o inelegible para su eliminación de acuerdo con la política de retención.

Al crear un backup, se puede establecer su política de retención. Posteriormente, se puede optar por conservar el backup durante un período más largo del que permite la política de retención o especificar que ya no es necesario el backup y desea que la política de retención lo gestione.

Información relacionada

El comando de actualización de backup de smo

Retención permanente de backups

Puede especificar que una copia de seguridad no sea elegible para su eliminación por parte de la política de retención, con el fin de conservar el backup de forma indefinida.

1. Para especificar que una copia de seguridad se conserve sin límite, escriba el siguiente comando: `smo backup update -profileprofile_name {-labellabel [data | -archivelogs] | -idid} -retain -unlimited`

Información relacionada

El comando de actualización de backup de smo

Asignar backups con una clase de retención específica

Los administradores de bases de datos pueden asignar una clase de retención específica por hora, día, semana o mes a los backups. La asignación de una clase de retención específica hace que los backups realizados bajo este cambio sean aptos para su eliminación.

1. Para asignar una clase de retención de copia de seguridad específica, introduzca este comando:SMO backup update -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | all} -retain [-Hourly | -Daily | -Weekly | -Monthly]

Cambiar el comportamiento predeterminado de la política de retención

Cuando caduca un backup según la política de retención, SnapManager determina si se elimina el backup según la configuración de retención. La eliminación de copias de seguridad es el comportamiento predeterminado. Puede cambiar este comportamiento predeterminado y liberar en su lugar las copias de seguridad no protegidas.

De forma predeterminada, SnapManager elimina o libera backups en función de si están protegidos o no de la siguiente manera:

- En el caso de los backups protegidos, SnapManager libera los backups locales cuando caducan.
- Para backups sin protección, SnapManager elimina los backups locales cuando caducan.

  Puede cambiar este comportamiento predeterminado.

Para los backups protegidos, SnapManager no tiene en cuenta lo siguiente a la hora de determinar si se debe eliminar la copia local:

- El backup en el almacenamiento secundario presenta un error o está en proceso de protección.

  Esto permite la transferencia de backups a un almacenamiento secundario antes de aplicar la normativa de retención.

- La copia se eliminó posteriormente del almacenamiento secundario.
  a. Acceda a la siguiente ubicación predeterminada:

     ubicación/propiedades de la instalación predeterminada de smo.config

  b. Edite el archivo smo.config.
  c. Establezca la propiedad retain.always FreeExpiredbackups en el archivo smo.config en true.

     Por ejemplo, retain.always FreeExpiredbackups = true

Información relacionada

El comando de actualización de backup de smo

Liberar o eliminar backups exentos de la política de retención

Los backups con clase de retención "ilimitada" no se pueden eliminar ni liberar directamente. Para eliminar o liberar estos backups, primero se debe asignar otra clase de retención, como por ejemplo cada hora, día, semana o mes. Para eliminar o liberar una copia de seguridad que esté exenta de la política de retención, primero debe actualizar la copia de seguridad para que sea elegible para su eliminación o su liberación.

1. Para actualizar el backup y poder borrarlo mediante la política de retención, escriba este comando: `smo backup update -profileprofile_name {-labellabel [data | -archivelogs] | -ididid} -retain [-hourly | -daily | -weekly | -monthly]`
2. Después de actualizar el backup de modo que sea apto para su eliminación, puede eliminar el backup o

liberar recursos de backup.

- Para eliminar la copia de seguridad, introduzca este comando: smo backup delete -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | -all}
- Para liberar los recursos de copia de seguridad, en lugar de eliminar la copia de seguridad, introduzca este comando:smo backup free -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | -all} [-force] [-dump] [-quiet | -verbose]

Información relacionada

El comando de actualización de backup de smo

Ver una lista de backups

Puede comprobar qué backups se han creado para un perfil y su estado de backup mediante el comando smo backup list. Para cada perfil, el comando muestra primero la información sobre el backup más reciente y, a continuación, continúa hasta que se muestra la información de todos los backups.

1. Introduzca el siguiente comando: `smo backup list -profileprofile_name [-delimitercharacter] [data | -archivelogs] [-quiet | -verbose]`

Información relacionada

El comando smo backup list

Ver los detalles de backup

Puede ver la información detallada sobre un backup concreto de un perfil mediante el comando smo backup show.

El comando smo backup show muestra la siguiente información de cada backup:

- El ID de la copia de seguridad
- Si la copia de seguridad se ha realizado correctamente o ha fallado
- Alcance de backup (completo, parcial, en línea o sin conexión)
- Modo de backup
- Estado de montaje
- La etiqueta de backup
- Comentar
- La fecha y la hora en que se inició y finalizó la operación
- Información sobre si se verificó el backup
- La clase de retención de copias de seguridad
- La base de datos y el nombre de host
- El número de cambio de sistema de punto de comprobación (SCN)
- El SCN de backup final (solo para backups en línea)
- Los espacios de tablas y los archivos de datos de la base de datos de la que se realizó un backup

- Los archivos de control de la base de datos de la que se realizó un backup
- Los registros de archivos de la base de datos de la que se realizó un backup
- El sistema de almacenamiento y los volúmenes donde se encuentran los archivos
- Las copias Snapshot realizadas y su ubicación
- El estado de los recursos de almacenamiento principales
- El estado de la protección de backup
- Una lista de copias en el almacenamiento secundario, con el formato backup_copy ID - node name
- Modo de backup

Si especifica la opción -verbose, se muestra la siguiente información adicional:

- Los clones del backup, si los hay
- Información de verificación
- Si se monta el backup, SnapManager muestra los puntos de montaje que están en uso

Para el backup de archivos de registro de archivos, se muestra la misma información que la del otro backup de base de datos excepto la siguiente información:

- SCN de punto de comprobación
- SCN de backup final
- Tablespace
- Archivos de control

Sin embargo, el backup del archivo de registro de archivos contiene la siguiente información adicional:

- El primer número de cambio del backup
- El siguiente número de cambio del backup
- Número de rosca
- Restablecer ID de registros
- Encarnación
- Nombre de archivo de registro
  a. Introduzca el siguiente comando: `smo backup show -profileprofile_name {-labellabel [data | -archivelogs] | -id id [-quiet | -verbose]`

Información relacionada

El comando smo backup show

Montar backups

SnapManager se encarga automáticamente del montaje de un backup para que el host esté disponible. También es posible montar backups en situaciones en las que se utilice una herramienta externa, como Oracle Recovery Manager (RMAN), para acceder a los archivos de la copia de seguridad.

Si utiliza RMAN, debe utilizar la operación de montaje para cambiar el estado de un backup (que permite el acceso) y la operación de desmontaje para cambiar el estado de un backup (que quita el acceso).

El comando smo backup Mount muestra una lista de rutas donde se han montado las copias Snapshot consistentes en el backup.

Puede usar la opción -from-secondary para montar el backup desde el almacenamiento secundario. Si no utiliza esta opción, SnapManager monta el backup desde el almacenamiento principal.

Debe especificar la opción -copy-id siempre que especifique la opción -from-secondary. Si existe más de un backup en el sistema de almacenamiento secundario, la opción -copy-id se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe utilizar para montar el backup.6

> Si se utiliza Data ONTAP en 7-Mode, es necesario especificar un valor válido para la opción -copy-id. Sin embargo, si utiliza Clustered Data ONTAP, la opción -copy-id no es necesaria.

Si va a montar un backup de base de datos en un host remoto, debe asegurarse de que las credenciales de Automatic Storage Management (ASM) sean las mismas en ambos hosts.

> Opcionalmente, es posible recoger los archivos de volcado después de una operación de montaje de backup exitosa o con errores.

1. Para montar un backup, introduzca el siguiente comando: `smo backup mount -profile profile_name {labellabel [data | -archivelogs] | -idid} [-host-host] [-from-secondary [-copy-id id]] [-dump] [-quiet | -verbose]`

Información relacionada

El comando de montaje de backup de smo

Desmontaje de backups

SnapManager desmonta automáticamente el backup para que no esté disponible para el servidor host. SnapManager también permite desmontar si se utiliza una herramienta externa, como Oracle Recovery Manager (RMAN), para acceder a los archivos de la copia de seguridad y para cambiar el estado del backup para quitar el acceso.

Si va a desmontar un backup de base de datos de un host remoto, debe asegurarse de que las credenciales de Automatic Storage Management (ASM) sean las mismas en ambos hosts.

Otra opción es recoger los archivos de volcado después de una operación de backup realizó una operación de desmontaje correcta o con errores.

La operación de desmontaje puede fallar en algún momento con un mensaje de error si el punto de montaje está ocupado, por ejemplo, --[ERROR] FLOW-11019 6598: Failure in Disconnect: SD-10046: No se puede desmontar el backup ya que el punto de montaje está ocupado con las siguientes rutas de montaje y PID: /Opt/NetApp/smo/mnt/-mnt-neuse_nfsvrdb_20120427052319903-Arch.

Debe identificar el PID de la sesión que tiene como resultado un fallo en la operación de desmontaje. Detenga la sesión ejecutando el siguiente comando: `kill pid`

Posteriormente, puede ejecutar la operación de desmontaje correctamente.

1. Introduzca el siguiente comando: `smo backup unmount -profile profile_name {labellabel [data | -archivelogs] | -idid} [-quiet | -verbose] -dump-force-verbose`

Información relacionada

El comando de desmontaje del backup de smo

Liberando backups

Es posible liberar backups, lo que elimina las copias Snapshot sin eliminar los metadatos de los backups. Esta función libera el espacio ocupado por la copia de seguridad. Puede utilizar el comando libre del backup de smo para liberar los backups.

Para que un backup pueda ser apto para liberar, debe asegurarse de lo siguiente:

- La copia de seguridad se ha realizado correctamente
- La copia de seguridad no se va a montar
- El backup no tiene clones
- El backup no se conservará mediante una política de retención ilimitada
- El backup no se ha liberado todavía

Si la protección está habilitada en el perfil y la política de protección contiene conexiones del nodo principal que usan una relación de mirroring, se eliminan copias Snapshot en el nodo principal cuando se libera un backup. Esas copias Snapshot también se eliminan de los nodos reflejados cuando se produce la próxima transferencia a almacenamiento secundario.

Cuando libera un backup protegido, SnapManager solicita que Protection Manager elimine las copias Snapshot locales para el backup. Si la operación libre de backup se realiza correctamente para los backups protegidos, Protection Manager elimina las copias de Snapshot de forma asíncrona.

Estado de protección	Estado local	De datos en cuanto al almacenamiento primario	Acción en el almacenamiento secundario	Explicación
No solicitado (protegido)	Existe	Libera el backup	No se requiere ninguna acción	SnapManager libera el backup local.
Liberado	No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada.	Sin proteger
Existe	Libera el backup	No se requiere ninguna acción	SnapManager libera el backup local aunque no haya copias en el almacenamiento secundario.	Liberado

Estado de protección	Estado local	De datos en cuanto al almacenamiento primario	Acción en el almacenamiento secundario	Explicación
No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada.	Protegido	Existe
Libera el backup	No se requiere ninguna acción; el backup en el secundario permanece	SnapManager libera el backup local. Las copias se conservan en el almacenamiento secundario.	Liberado	No se requiere ninguna acción

Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de backup libre exitosa o con errores.

1. Introduzca el siguiente comando: smo backup free -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | -all} -force [-dump] [-quiet] [-force]

Información relacionada

El comando libre de backup de smo

Eliminar backups

Debe eliminar backups cuando ya no los necesite, lo que libera el espacio que estos backups ocupan. Si elimina los backups, reducirá la posibilidad de alcanzar el límite de 255 copias snapshot por volumen.

- Debe asegurarse de que el backup no se haya usado para crear un clon.

Cuando se elimina un backup protegido, SnapManager elimina el backup del almacenamiento secundario y el repositorio de SnapManager. En la siguiente tabla, se muestran las acciones emprendidas en el almacenamiento primario y secundario al eliminar un backup local:

Estado de protección	Estado local	De datos en cuanto al almacenamiento primario	Acción en el almacenamiento secundario	Explicación
No solicitado (protegido)	Existe	Elimina las copias Snapshot	No se requiere ninguna acción	SnapManager eliminará el backup local.

Estado de protección	Estado local	De datos en cuanto al almacenamiento primario	Acción en el almacenamiento secundario	Explicación
Liberado	No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada. Si se elimina un backup liberado, los metadatos del backup se eliminan del repositorio.	Sin proteger
Existe	Elimina las copias Snapshot	No se requiere ninguna acción	SnapManager elimina el backup local tanto si se ha protegido como si no.	Liberado
No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada. Si se elimina un backup liberado, los metadatos del backup se eliminan del repositorio.	Protegido	Existe
Elimina las copias Snapshot	SnapManager elimina el backup en el almacenamiento secundario	SnapManager elimina el backup local y las copias secundarias.	Liberado	No se requiere ninguna acción

Si intenta eliminar un backup que está protegido por el almacenamiento secundario, es posible que las copias de Snapshot se marquen para eliminarse y, posteriormente, Protection Manager las elimina.

Puede eliminar backups retenidos de forma ilimitada sin cambiar la clase de retención.

Opcionalmente, es posible recoger los archivos de volcado después de la operación de eliminación de backup exitosa o con errores.

Si desea eliminar los backups de registros de archivos, debe comprobar la duración de retención establecida para el backup de registros de archivos. Si el backup de registros de archivos se encuentra dentro de la duración de retención y se requieren archivos de registro de archivos para la recuperación de una base de datos restaurada, no se puede eliminar el backup de registros de archivos.

1. Para verificar que las operaciones se han completado, introduzca el siguiente comando: smo operation list -profileprofile_name-quiet-verbose
2. Para eliminar una copia de seguridad, introduzca el siguiente comando:copia de seguridad de smo delete -profile profile_name [-label label label label [data | -archivvelogs] | -idid | -all] [-force] [-dump] [-quiet | -verbose]

Utilice la opción -force para forzar la eliminación del backup. Forzar la eliminación de un backup que tenga operaciones incompletas podría dejar el backup en estado incoherente.

Programación de backups de bases de datos

SnapManager (3.2 o posterior) para Oracle permite programar backups de bases de datos de forma regular durante las horas de menor actividad para mantener un alto rendimiento. Para programar un backup, puede crear un perfil, que incluya la información de la base de datos y la política de retención, y luego establecer programaciones para el backup.

> Debe programar los backups como usuario raíz o como usuario de Oracle. Si intenta programar los backups como usuario no existente, SnapManager muestra un mensaje de error: Invalid user: username: No puede crear un backup de programación para un usuario determinado

A continuación, se muestran algunas de las tareas relacionadas con la programación:

- Programar un backup de base de datos para que se realice por hora, día, semana, mes o una sola vez.
- Ver una lista de los backups programados asociados con un perfil.
- Actualizar una copia de seguridad programada.
- Suspender temporalmente una programación.
- Reanude la programación suspendida.
- Eliminar una programación.

> La casilla de verificación **operación del menú Ejecutar ahora** está desactivada cuando se está ejecutando una copia de seguridad programada para esa programación.

Creando programaciones de backup

Es posible programar un backup en el momento y la frecuencia que sean adecuados para sus datos y entorno.

En SnapManager 3.2 para Oracle, es posible programar los backups de los archivos de registro de archivos por separado. Sin embargo, debe utilizar el perfil que ha creado para separar los archivos de registro de archivos.

Si programó los backups de los archivos de datos y los archivos de registro de archivos al mismo tiempo, SnapManager creará primero el backup de los archivos de datos.

Si selecciona el intervalo de programación como -onetimeonly, todas las opciones de eliminación estarán disponibles. Si selecciona un intervalo de programación distinto de -onetime only, no se admiten las opciones de eliminación -until-SCN y -until-date y se muestra el siguiente mensaje de error: La opción de eliminación del registro de archivado especificada, -until-scn o -until-date para el intervalo por hora de programación no es válida. Especifique la opción -onetimeonly para el intervalo de programación o pine los registros de archivo utilizando cualquiera de las opciones all, o -before {-months | -days | -weeks| -hours}.

Cuando se produce una conmutación por error en un entorno de multiprocesamiento de clústeres de alta disponibilidad (HACMP), debe reiniciar el servidor SnapManager para Oracle para que la dirección de servicio (virtual) se asigne al host activo y las programaciones de SnapManager se ajusten al host SnapManager

activo. Puede agregar esta información en las secuencias de comandos de conmutación por error de HACMP de preprocesamiento o después del procesamiento.

> Si existe el mismo perfil y nombre de programación en otro repositorio, no se inicia la operación de programación de backup en ese repositorio. Se cerrará la operación con el siguiente mensaje: Ya se está ejecutando.

1. Introduzca el siguiente comando: programación de smo create -profile_name {[-full {-online | -offline | -auto}[-retain [-hora | -diario | -semanal | -mensual | -ilimitado] [-verify] | [-data [-filesfiles [ficheros] | [-tablespaces [-auto-comentarios]] {-online | -unoffline | -auto_protecs | -unt] | -tnow [-tnough]] | -tnough] | -tnough [-tnough]] | -tnough] [-tnough] | -tnual [-tnual]]] -NoProtect] [-backup-destinpath1 [,[path2] [-exclude-destinpath1 [,path2] [-DEScommentelogs{-all | -unSCNuntilSCN | -until-croneyi-MM-dd HH:mm:ss | -before {-mesh | -weeks | -days | -dunch-prunch-time-prunit] -unit_prunch-time-time] -unit_prunit_prunit_prunit] -unit_prunit-time-time-time [_prunit] -unit_prunit_prunit_prunit] <yyyy-MM-dd HH:mm>

Si desea…	Realice lo siguiente…
Programar una copia de seguridad de una base de datos en línea o sin conexión	Especifique -offline o -online para programar un backup de la base de datos sin conexión o en línea. Si especifica las opciones, no se puede utilizar -auto.
Deje que SnapManager gestione la programación de una base de datos independientemente de si está en línea o sin conexión	Especifique -auto. Si especifica -auto, no puede utilizar --offline o -online.
Programar una copia de seguridad de archivos de datos	Especifique -data -files para enumerar los archivos separados por comas. Por ejemplo, utilice los nombres de archivo f1,f2,f3.
Programar una copia de seguridad parcial de tablespaces específicos	Especifique -tablespaces para enumerar los tablespaces separados por comas. Por ejemplo, utilice ts1,ts2,ts3.
Programar copia de seguridad de archivos de registro de archivo	Especifique lo siguiente: • -archivelogs para programar la copia de seguridad de los archivos de registro de archivo • -backup-dest para programar los destinos de archivos de registro de archivos que se incluirán en el backup • -exclude-dest para programar los destinos de registro de archivos que se excluirán del backup

Si desea…	Realice lo siguiente…
Especifique los valores de la clase de retención	Especifique -retain e indique si el backup debe conservarse de acuerdo con una de las siguientes clases de retención: • -cada hora • - diariamente • -semanal • -mensual • -El valor predeterminado de SnapManager ilimitado es cada hora.
Programar la eliminación de archivos de registro de archivos	Especifique lo siguiente: **-Prunelogs para afinar los archivos de registro de archivos mientras se programa una copia de seguridad** -prune-dest para especificar el destino de registro de archivos desde el que se recortan los archivos de registro de archivos
Incluya un nombre para el horario	Especifique -schedule-nombre.
Programar copia de seguridad de la base de datos en un intervalo de tiempo específico	Especifique la opción INTERVAL y seleccione el intervalo de tiempo entre las siguientes, mediante el cual deben crearse los backups: • -cada hora • - diariamente • -semanal • -mensual • -untimeonly

Si desea…	Realice lo siguiente…
Configurar un horario	Especifique -cronstring e incluya las siguientes siete subexpresiones que describen la opción individual: • 1 se refiere a segundos. • 2 se refiere a minutos. • 3 se refiere a horas. • 4 se refiere a un día en un mes. • 5 se refiere al mes. • 6 se refiere a un día en una semana. • (Opcional) 7 se refiere al año. **Nota:** Si programó su copia de seguridad con diferentes horas en -cronstring y -start-time, entonces la programación de la copia de seguridad se sobrescribe y se activa por la -start-time.
Agregar un comentario sobre el programa de copia de seguridad	Specify -schedule-comment seguido de la cadena de descripción.
Especifique la hora de inicio de la operación de programación	Especifique -start-time en el formato yyyy-mm-dd hh:mm.
Cambiar el usuario de la operación de copia de seguridad programada mientras se programa la copia de seguridad	Especifique -runasuser. La operación se ejecuta como el usuario (usuario raíz o usuario de Oracle) que creó la programación. Sin embargo, puede utilizar su propio ID de usuario si tiene credenciales válidas tanto para el perfil de base de datos como para el host.
Active una actividad de tareas previas o posteriores a la tarea de la operación de programación de copia de seguridad mediante el archivo XML de especificación de tareas previas y posteriores	Especifique la opción -taskspec y proporcione la ruta absoluta del archivo XML de la especificación de la tarea para realizar un preprocesamiento o una actividad de post-procesamiento que tenga lugar antes o después de la operación de programación de copia de seguridad.

Actualizar una programación de backup

Puede ver una lista de operaciones programadas y actualizarlas si es necesario. Puede actualizar la frecuencia de programación, la hora de inicio de la programación, la expresión cronstring y el usuario que programó la copia de seguridad.

1. Para actualizar la programación de un backup, escriba el siguiente comando: `smo schedule update -profile profile_name-schedule-nameschedulename [-schedule-commentschedule comment] -interval {-hourly | -daily | -weekly | -monthly | -onetimeonly} -start-timestarttime-cronstringcronstring-runasuserrunasuser [-quiet |`

```
-verbose]
```

Ver una lista de operaciones programadas

Es posible ver una lista de las operaciones programadas para un perfil.

1. Para mostrar la información sobre el funcionamiento programado, escriba el siguiente comando: `smo schedule list -profile profile_name[-quiet | -verbose]`

Suspensión de programaciones de backup

SnapManager permite suspender una programación de backup hasta que se reanude la programación de backup.

Puede suspender las programaciones activas. Si intenta suspender la programación de backup que ya se encuentra suspendida, es posible que aparezca el mensaje de error "no se puede suspender: Schedule <schedulename> ya en estado de suspensión".

1. Para suspender temporalmente la programación del backup, introduzca este comando: `smo schedule suspend -profile profile_name-schedule-nameschedulename [-quiet | -verbose]`

Reanudar programaciones de backup

Los administradores tienen la opción de reanudar la programación de backup suspendida.

Si intenta reanudar las programaciones activas, es posible que aparezca el mensaje de error "no se puede reanudar: Schedule <schedulename> ya en estado de reanudación".

1. Para reanudar la programación de backup suspendida, introduzca este comando: smo schedule resume -profile profile_name-schedule-namesetnamesetName [-quiet | -verbose]

Eliminación de programaciones de backup

Es posible eliminar programaciones de backup cuando ya no sean necesarias.

1. Para eliminar la programación de copia de seguridad, introduzca este comando: smo schedule delete -profile_name-schedule-namesetnameName [-quiet | -verbose]

Restaurar backups de base de datos

SnapManager para Oracle le permite restaurar una base de datos al estado que tenía cuando se tomó una copia Snapshot. Además del proceso de restauración basada en archivos, SnapManager admite la tecnología de restauración rápida basada en volúmenes, lo que reduce el tiempo de restauración de forma significativa en comparación con otros métodos de recuperación. Debido a que los backups se crean con más frecuencia, se reduce el número de registros que se debe aplicar, lo que reduce el tiempo medio de recuperación (MTTR) de una base de datos.

A continuación, se muestran algunas de las tareas que se pueden realizar en relación con la restauración y la

recuperación de datos en bases de datos:

- Realizar una restauración basada en archivos o una restauración basada en volúmenes, que es el método más rápido de restaurar backups de base de datos y es el valor predeterminado que utiliza SnapManager.
- Restaure todo el backup o parte del mismo.

  Cuando se restaura una parte de la misma, se especifica un grupo de espacios de tablas o un grupo de archivos de datos. También puede restaurar los archivos de control junto con los datos o solo los propios archivos de control.

- Recupere los datos en función de un momento específico o de todos los registros disponibles, que almacena la última transacción comprometida con la base de datos.

  El punto en el tiempo puede ser un número de cambio de sistema (SCN) de Oracle o una fecha y hora (aaaa-mm-dd:hh:mm:ss). SnapManager utiliza el reloj de 24 horas.

- Restauración desde backups en el almacenamiento principal (backups locales).
- Restaurar y recuperar la copia de seguridad mediante SnapManager, o usar SnapManager para restaurar la copia de seguridad y utilizar otra herramienta, como Recovery Manager (RMAN), para recuperar los datos.
- Restaurar backups desde ubicaciones alternativas.
- Restaure los backups protegidos del almacenamiento secundario (backups remotos) y desde una ubicación alternativa mediante el archivo de especificación de restauración.

Puede restaurar una copia de seguridad realizada por una versión anterior de SnapManager utilizando SnapManager 3.0 y versiones posteriores.

SnapManager también permite restaurar las bases de datos de gestión automática de almacenamiento (ASM). Un grupo de discos ASM puede compartirse con varias bases de datos. Por lo tanto, no es posible revertir a una copia Snapshot más antigua del grupo de discos, ya que revería todas las bases de datos. Las soluciones tradicionales de operaciones de restauración pasan por el host y requieren que todos los bloques que conforman la base de datos se muevan del sistema de almacenamiento al host y, después, al sistema de almacenamiento. SnapManager libera esta sobrecarga, ya que permite restaurar solo los datos necesarios en el grupo de discos de ASM sin pasar por el host.

Los administradores pueden realizar operaciones de restauración o recuperación mediante la interfaz gráfica de usuario (GUI) de SnapManager o mediante la interfaz de línea de comandos (CLI).

Información relacionada

Realizar backups de bases de datos

El comando smo backup restore

Qué es la restauración de base de datos

SnapManager permite realizar operaciones de backup y restauración basadas en volúmenes o archivos.

En la siguiente tabla se describen los métodos de restauración:

Proceso de restauración	Detalles
Restauraciones rápidas basadas en volúmenes (desde el almacenamiento primario)	SnapManager restaura los archivos de datos de una base de datos mediante la restauración de un volumen completo. Este proceso predeterminado es el método más rápido para restaurar la base de datos.
Restauraciones basadas en archivos	Restauración de sistema de archivos completo en el almacenamiento (desde el principal o el secundario): SnapManager realiza una restauración completa del número de unidad lógica (LUN).
Restauración de archivos del lado del almacenamiento: SnapManager realiza una restauración de snap de archivos única (SFSR) en un entorno NAS o una restauración snap de archivos parcial (PFSR) en un entorno de administración automática de almacenamiento (ASM). En SFSR, se restauran los archivos o las LUN que representan los objetos protegidos. Se realiza un PFSR desde la copia de seguridad local si los detalles del sistema de archivos y el diseño del sistema de archivos no han cambiado desde que se realizó la copia de seguridad anterior.	Restauración de copias de archivos del lado del host (desde el principal o secundario): SnapManager clona el backup local con una LUN o un FlexClone. El clon se monta y, a continuación, SnapManager copia los archivos host del clon en el sistema de archivos activo.

Aunque el valor predeterminado es el proceso de restauración rápida, los administradores pueden elegir cualquiera de los dos tipos. Durante el proceso de restauración rápida, SnapManager ofrece información sobre las condiciones en las que no se puede completar el proceso de restauración rápido y sobre las que puede afectar a la rápida restauración, pero qué administradores pueden ignorar si deciden continuar con el proceso.

> No es posible restaurar un backup desde el almacenamiento secundario si el backup también existe en el almacenamiento principal.

Cuando se completa la operación de restauración rápida, SnapManager realiza las siguientes tareas:

- Libera backups más recientes (que se toman después de la restauración del backup) en el mismo perfil, ya que sus copias Snapshot ya no existen en el almacenamiento principal.
- Elimina todas las copias Snapshot para backups del mismo perfil que tenía cualquier copia Snapshot eliminada automáticamente por el proceso de restauración rápida.

  Esto evita que los backups se liberen parcialmente. Por ejemplo, primero se creó Backup_A y, a continuación, se creó Backup_B. Cada uno tiene una copia snapshot para los archivos de datos y uno para los registros de archivos. Una vez que SnapManager restaura Backup_A mediante el proceso de restauración rápida, SnapManager elimina automáticamente la copia snapshot de los archivos de datos de Backup_B. Dado que el registro de archivos no se restaura en el proceso de restauración rápida, SnapManager debe eliminar la copia Snapshot de los registros de archivos de Backup_B una vez completado el proceso de restauración rápida.

Restauración rápida

La restauración rápida o la restauración basada en volúmenes se denominan porque es el método de restauración más rápido posible. Todo el volumen del sistema de almacenamiento vuelve a una copia Snapshot. En el nivel de almacenamiento, esta restauración es casi instantánea. No obstante, al restaurar un volumen, se pueden producir las siguientes consecuencias negativas y, por lo tanto, se debe usar con precaución:

- Se revierte todo el volumen en el lado del almacenamiento, incluidos los siguientes:
  - Archivos que no se consideraron como parte de la copia de seguridad
  - Otros archivos, sistemas de archivos o LUN en el volumen
- Se eliminan todas las copias Snapshot que se crearon después de la copia Snapshot en la que se revierte el volumen.

  Por ejemplo, ya no puede restaurar el backup del martes si el backup del lunes fue restaurado.

- Las relaciones con los sistemas de almacenamiento secundario se interrumpen si la copia Snapshot restaurada es más antigua que la copia Snapshot básica de la relación.

Restauración de todo el sistema de archivos en el lado del almacenamiento

Se realiza una restauración de sistema de archivos completo en el lado del almacenamiento cuando no es posible realizar una restauración de volumen, pero es posible restaurar todo el sistema de archivos en el sistema de almacenamiento.

Cuando se realiza una restauración del sistema de archivos en el almacenamiento, se produce lo siguiente:

- En un entorno SAN, todas las LUN utilizadas por el sistema de archivos (y el grupo de volúmenes subyacente, si las hubiera) se restauran en el sistema de almacenamiento.
- En un entorno NAS, todos los archivos del sistema de archivos se restauran en el sistema de almacenamiento.

  En los entornos NAS, este mecanismo de restauración no proporciona ventajas adicionales con respecto a la restauración de archivos del almacenamiento.

Cuando se realiza una restauración del sistema de archivos en el almacenamiento, se produce lo siguiente, según la ubicación del almacenamiento:

- Cuando las restauraciones de SnapManager desde sistemas de almacenamiento primario, se restauran las LUN (SAN) o los archivos (NAS) mediante SFSR.
- Cuando SnapManager restaura desde sistemas de almacenamiento secundario, los LUN (SAN) o los archivos (NAS) se copian desde los sistemas de almacenamiento secundario de vuelta al sistema de almacenamiento primario a través de la red.

Como el sistema de archivos se restaura por completo, se revierten los archivos que no sean parte del backup. Se requiere una anulación si los archivos, que no forman parte de la restauración, se encuentran en el sistema de archivos que se está restaurando.

Restauración de archivos del lado del almacenamiento

En ocasiones, se realiza una restauración de archivos en el lado del almacenamiento cuando no se puede realizar una restauración del sistema de archivos en el lado del almacenamiento. En una restauración de

archivos del almacenamiento, los archivos individuales de un sistema de archivos se restauran directamente en los sistemas de almacenamiento.

Este tipo de restauración solo se puede realizar en entornos NFS.

En los entornos ASM, la restauración de archivos en el lado del almacenamiento solo se puede realizar si se aplican las siguientes condiciones:

- Las extensiones de archivos subyacentes no han cambiado desde que se realizó la copia de seguridad (por ejemplo, no se cambió el tamaño del archivo y no se produjo el reequilibrio del disco).
- Se restaura a partir de sistemas de almacenamiento primarios. (No admite la restauración desde sistemas de almacenamiento secundarios).

Cuando se realiza una restauración de archivos en el almacenamiento, se produce lo siguiente:

- Cuando SnapManager restaura archivos NFS de sistemas de almacenamiento primario, se restauran los archivos individuales mediante SFSR.
- Cuando SnapManager restaura archivos NFS desde sistemas de almacenamiento secundario, los archivos individuales se vuelven a copiar en el sistema de almacenamiento primario a través de la red de almacenamiento.
- Cuando se restauran los archivos ASM de sistemas de almacenamiento primario, los archivos individuales se restauran únicamente los bytes de las LUN subyacentes asociadas con los archivos que se van a restaurar (el resto de los bytes de las LUN permanecen intactos). La tecnología del sistema de almacenamiento utilizada para restaurar parcialmente las LUN se denomina PFSR.

Restauración de archivos del lado del host

Una restauración de copias de archivos en el lado del host se usa como último recurso en entornos SAN cuando no se pueden realizar restauraciones rápidas, restauraciones del sistema de archivos en el lado del almacenamiento y restauración de archivos en el lado del almacenamiento.

Una restauración de copias de archivos del host implica las siguientes tareas:

- Clonar el almacenamiento
- Conectar el almacenamiento clonado al host
- Copiar archivos de los sistemas de archivos clonados de nuevo en los sistemas de archivos activos
- Desconectar el almacenamiento de clones del host
- Eliminar el almacenamiento del clon

Cuando se restaura desde el almacenamiento secundario, SnapManager intenta primero restaurar los datos directamente desde el sistema de almacenamiento secundario al sistema de almacenamiento primario (sin afectar el host). Si SnapManager no puede realizar este tipo de restauración (por ejemplo, si los archivos no forman parte de la restauración existen en un sistema de archivos), SnapManager realizará una restauración de copia de archivos del lado del host. SnapManager tiene dos métodos para realizar una restauración de copia de archivos en el lado del host desde el almacenamiento secundario. El método SnapManager selecciona se configura en el archivo smo.config.

- Directo: SnapManager clona los datos del almacenamiento secundario, monta los datos clonados del sistema de almacenamiento secundario en el host, y después copia los datos del clon en el entorno activo. Esta es la directiva de acceso secundaria predeterminada.
- Indirecto: SnapManager copia primero los datos en un volumen temporal del sistema de almacenamiento

primario y, a continuación, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo. Esta normativa de acceso secundario se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Las restauraciones mediante este método tardan el doble de tiempo que la normativa de acceso secundario directo, ya que se realizan dos copias de los datos.

La decisión de utilizar el método directo o indirecto se controla mediante el valor del parámetro restore.secondaryAccessPolicy del archivo de configuración smo.config. El valor predeterminado es directa.

Directrices sobre cuándo utilizar la restauración rápida

Existen reglas específicas que se aplican para usar la restauración rápida con el fin de lograr un rendimiento óptimo de la restauración. En algunos casos, no se puede utilizar una restauración rápida.

Para lograr un rendimiento de restauración óptimo (restauración de volúmenes o restauración de grupos de discos completos), se deben cumplir las siguientes reglas:

- Solo las restauraciones completas de backups completos pueden ser válidas para una restauración rápida.
- Solo los archivos de datos pueden optar a una restauración rápida.
- Los archivos de datos deben ser los únicos archivos de un volumen que puedan optar a una restauración rápida.

  Aunque los archivos de datos temporales pueden residir en el volumen, los archivos de control, los registros, los archivos pfiles u otros archivos deben residir en un volumen independiente de los archivos de datos. Debe configurar una base de datos de Oracle con archivos de datos en un volumen aparte de los archivos de control, registros archivados y archivos de registro en línea.

- Los archivos de datos de una sola base de datos deben estar presentes en el volumen.
- Se pueden utilizar varios sistemas de archivos, pero los archivos de dichos sistemas de archivos deben ser archivos de datos para una única base de datos.
- Para las bases de datos de ASM, cada base de datos debe utilizar su propio grupo de discos de ASM y la base de datos de ASM no puede compartir almacenamiento con ninguna otra base de datos de ASM.

> Para comprobar si un backup creado previamente se puede restaurar mediante una restauración rápida, puede utilizar la opción -preview del comando smo backup restore.

El proceso de restauración rápida no se puede utilizar en los siguientes casos:

- En backups parciales
- En backups desde el almacenamiento secundario si el backup también existe en el almacenamiento primario

  No es posible restaurarlos mediante la restauración basada en archivos o volúmenes.

- En backups protegidos con SnapVault

  El proceso de restauración rápida no se puede utilizar para backups creados con anterioridad al último backup protegido. No obstante, se puede utilizar el proceso de restauración rápida de los backups creados después del último backup protegido. Considere, por ejemplo, los backups A, B y C. B es el último backup a transferir a almacenamiento secundario mediante SnapVault. Puede restaurar B y C rápidamente, pero

no puede restaurar A rápidamente porque se creó antes que la última copia de seguridad protegida. SnapVault necesita una SnapVault básica para calcular la diferencia de tiempo y enviar al almacenamiento secundario la próxima vez que se transfiere un backup al almacenamiento secundario. El último backup protegido actúa como la copia Snapshot de referencia. Por lo tanto, si se utiliza el proceso de restauración rápida, SnapVault no podrá reconocer la línea de base.

- Clones de FlexClones o LUN que utilizan copias de Snapshot que se crearon después de la copia Snapshot en la que se está recreando el volumen

  Por ejemplo, los clones pueden ser el resultado de un backup posterior que SnapManager está montado o clonado.

- LUN que no forman parte de la copia snapshot activa de SnapDrive

No es posible realizar una restauración rápida junto con otros tipos de restauraciones para la misma copia de seguridad. Por ejemplo, si se puede restaurar un volumen de datos mediante el proceso de restauración rápida pero no puede otro volumen de datos, ninguno de los cuales se restaurará mediante el proceso de restauración rápida. En este caso, es posible elegir una restauración basada en archivos.

Además, debe tener en cuenta los puntos siguientes sobre las restauraciones de bases de datos:

- SnapManager nunca restaura registros de archivos ni registros de reconstrucción, pero monta la copia de seguridad de archivos de registro de archivos y los utiliza para la recuperación.
- SnapManager nunca restaura los archivos de control mediante la restauración de volúmenes.
- Si desea restaurar archivos de control y archivos de datos, SnapManager realiza la restauración en dos pasos.

  SnapManager restaura los archivos de control primero y después los archivos de datos.

- Si SnapManager encuentra archivos temporales en el mismo volumen que los archivos de espacio de tabla estándar, no es necesario emitir una sobrescritura para realizar una restauración a nivel de volumen.

  Después de una restauración de volumen, el espacio de tabla TEMPORAL vuelve a estar en línea.

Información relacionada

Diseños generales de bases de datos y configuraciones de almacenamiento recomendados

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Ventajas e inconvenientes del uso de la restauración rápida

Los administradores de bases de datos deben conocer las ventajas y desventajas que supone el uso de restauraciones rápidas basadas en volúmenes.

La restauración de backups de base de datos mediante restauraciones rápidas ofrece las siguientes ventajas:

- Las restauraciones basadas en volúmenes reducen el tiempo necesario para restaurar backups.
- SnapManager ofrece comprobaciones rápidas de los requisitos para las restauraciones. SnapManager analiza el backup de la base de datos y muestra información sobre si puede ejecutar la restauración basada en volúmenes.
- Puede obtener una vista previa de la operación de restauración y decidir si continuar con la ruta recomendada o anular la recomendación con el proceso seleccionado.

La restauración de backups de base de datos mediante restauraciones rápidas presenta las siguientes desventajas:

- Se revierte todo el sistema de archivos, incluidos los archivos que no se consideraron parte de la copia de seguridad. También se revierten otros archivos, sistemas de archivos o LUN del volumen.
- SnapManager quita todas las copias Snapshot que se realizaron después de que la Snapshot a la que se está revirtiendo. De hecho, pierde el historial después de la fecha de la copia Snapshot. Por ejemplo, no puede restaurar la copia de seguridad del martes si ya ha restaurado la copia de seguridad del lunes.

Puede evitar estas desventajas si sigue estas recomendaciones:

- Optimice el diseño de la base de datos de acuerdo con prácticas recomendadas.
- Proteger los backups en el almacenamiento secundario. Sin embargo, si elimina copias Snapshot del almacenamiento primario, no puede usar restauraciones rápidas para restaurarlas desde el almacenamiento secundario.

Rápidas comprobaciones de cumplimiento de la restauración

Cuando decide realizar una restauración rápida de un backup, SnapManager realiza en primer lugar una comprobación de idoneidad para determinar si puede utilizar el proceso de restauración rápida.

SnapManager ofrece los siguientes tipos de comprobaciones:

- Comprobaciones obligatorias: SnapManager puede realizar el proceso de restauración rápida sólo si se cumplen todas las condiciones en esta fase de comprobación.
- Comprobaciones anulables: Si las condiciones de esta comprobación fallan, los administradores pueden anular la comprobación para forzar un proceso de restauración rápida. Sin embargo, debe anular estas comprobaciones con precaución.

En la siguiente tabla se enumeran los problemas que puede encontrar e indican si la comprobación de elegibilidad de la restauración rápida puede anularse:

Problema	Se requiere pasar	Detalles
ACFS, Voting Disk o OCR está presente en el grupo de discos ASM en 11gR2	Sí	No se puede realizar una restauración rápida. Resolución: Ninguna No se puede anular.
Solo los backups creados con SnapManager 3.0 o posterior se pueden restaurar rápidamente	Sí	No se puede anular.
Sólo se pueden restaurar rápidamente las copias snapshot creadas con SnapDrive para UNIX 4.0 o posterior	Sí	No se puede anular.

Problema	Se requiere pasar	Detalles
El volumen es un volumen raíz	Sí	El volumen que se restaura es un volumen raíz en el sistema de almacenamiento. Resolución: No utilice el volumen raíz en el sistema de almacenamiento. No se puede anular.
La restauración de volúmenes no está disponible en Windows	Sí	El volumen que se restaura es un volumen raíz en el sistema de almacenamiento. Resolución: Ninguna No se puede anular.
Se deshabilita la restauración de volumen	Sí	Se deshabilitó la restauración de volúmenes. Resolución: Active la restauración de volúmenes seleccionando diferentes opciones al iniciar la restauración. En la interfaz de línea de comandos, no utilice -fast -off. No se puede anular.

Problema	Se requiere pasar	Detalles
Controle los archivos y los archivos de datos del mismo volumen	Sí	Para los backups en línea, los archivos de control y los archivos de datos no pueden estar en el mismo volumen porque SnapManager toma dos copias snapshot del volumen (una en la que los archivos de datos son consistentes en el modo de backup dinámico, y uno en el que los archivos de control de copia de seguridad son consistentes después de completar el modo de copia de seguridad en caliente). La restauración del volumen volverá a la primera copia snapshot, lo que elimina la segunda copia snapshot que contiene los archivos de control de backup. Si se produce una restauración solo de archivos de datos, los archivos de control se restauran en un estado incoherente, SnapManager restaura el archivo de control de backup y abre la base de datos con la opción reaslogs, lo cual no es el comportamiento deseado. Resolución: Migre los archivos de control y los archivos de datos a sistemas de archivos independientes que no compartan el mismo volumen subyacente. Esto no ayuda a la restauración en la cual la comprobación falló, pero sí a las operaciones de restauración de backup futuras. No se puede anular.

Problema	Se requiere pasar	Detalles
Los registros de archivo y los archivos de datos no deben existir en el mismo volumen	Sí	Los registros de archivo de bases de datos y los archivos de datos residen en sistemas de archivos respaldados por el mismo volumen del sistema de almacenamiento. Si se ejecutó una restauración de volumen, SnapManager no puede abrir la base de datos después de la restauración de un backup en línea debido a que el archivo de registro archivado que se escribe una vez que la base de datos se desconecta del modo de backup dinámico no está disponible. Además, no podría avanzar por transacciones posteriores que podrían haber estado en los archivos de registro de archivos. Resolución: Migre los registros de archivos y los archivos de datos a sistemas de archivos independientes que no compartan el mismo volumen de sistema de almacenamiento subyacente. Esto no ayuda a la restauración en la cual la comprobación falló, pero sí a las operaciones de restauración de backup futuras. No se puede anular.

Problema	Se requiere pasar	Detalles
Los registros en línea y los archivos de datos no deben existir en el mismo volumen	Sí	Los registros de recuperación y los archivos de datos en línea de la base de datos residen en sistemas de archivos respaldados por el mismo volumen del sistema de almacenamiento. Si se realizó una restauración de volumen, la recuperación no puede utilizar los registros de recuperación en línea porque se habrían revertido. Solución: Migre los redo logs y los archivos de datos en línea a sistemas de archivos independientes que no compartan el mismo volumen de sistema de almacenamiento subyacente. Esto no ayuda a la restauración en la cual la comprobación falló, pero sí a las operaciones de restauración de backup futuras. No se puede anular.

Problema	Se requiere pasar	Detalles
Se revierten los archivos del sistema de archivos que no formen parte del ámbito de restauración	Sí	Los archivos visibles en el host, excepto los archivos que se van a restaurar, existen en un sistema de archivos del volumen. Si se realizó una restauración rápida o una restauración de sistema de archivos en el lado del almacenamiento, los archivos visibles en el host se revertirían a su contenido original al crear la copia Snapshot. Si SnapManager descubre 20 o menos archivos, se enumeran en la comprobación de elegibilidad. De lo contrario, SnapManager muestra un mensaje que debería investigar el sistema de archivos. Resolución: Migre los archivos no utilizados por la base de datos a un sistema de archivos diferente que utilice un volumen diferente. También puede eliminar los archivos. Si SnapManager no puede determinar el propósito del archivo, puede anular el fallo de comprobación. Si se anula la comprobación, se revierten los archivos que no estén en el ámbito de restauración. Anule esta comprobación sólo si está seguro de que al revertir los archivos no se afectará negativamente a nada.

Problema	Se requiere pasar	Detalles
Se revierten los sistemas de archivos del grupo de volúmenes especificado que no formen parte del alcance de restauración	No	Hay varios sistemas de archivos en el mismo grupo de volúmenes, pero no se solicitan que se restauren todos los sistemas de archivos. La restauración del sistema de archivos del almacenamiento y la restauración rápida no se pueden usar para restaurar sistemas de archivos individuales dentro de un grupo de volúmenes, ya que las LUN que utiliza el grupo de volúmenes contienen datos de todos los sistemas de archivos. Todos los sistemas de archivos de un grupo de volúmenes deben restaurarse a la vez para utilizar una restauración rápida o una restauración del sistema de archivos del lado del almacenamiento. Si SnapManager descubre 20 archivos o menos, SnapManager los enumera en la comprobación de elegibilidad. De lo contrario, SnapManager proporciona un mensaje que debería investigar el sistema de archivos. Resolución: Migre los archivos que no utiliza la base de datos a un grupo de volúmenes diferente. Otra opción es eliminar los sistemas de archivos del grupo de volúmenes. Puede anular.

Problema	Se requiere pasar	Detalles
Se revierten los volúmenes de host de un grupo de volúmenes especificado que no forman parte del alcance de restauración	No	Varios volúmenes de host (volúmenes lógicos) están en el mismo grupo de volúmenes, pero no todos los volúmenes de host se solicitan que se restauren. Esta comprobación es similar a los sistemas de archivos del grupo de volúmenes que no forman parte del ámbito de restauración se revertirá excepto que los demás volúmenes de host del grupo de volúmenes no se montan como sistemas de archivos en el host. Resolución: Migre los volúmenes de hosts que utiliza la base de datos a otro grupo de volúmenes. O bien, elimine los otros volúmenes de host del grupo de volúmenes. Si anula la comprobación, se restauran todos los volúmenes de host del grupo de volúmenes. Anule esta comprobación solo si tiene la seguridad de que la reversión de los otros volúmenes de host no afecta negativamente en nada.
Las extensiones de archivo han cambiado desde la última copia de seguridad	Sí	No se puede anular.

Problema	Se requiere pasar	Detalles
Los LUN asignados en el volumen no forman parte del ámbito de restauración se revierten	Sí	Las LUN distintas de las solicitadas para restaurar en el volumen están actualmente asignadas a un host. No se puede realizar una restauración de volúmenes porque otros hosts o aplicaciones que utilizan estos LUN se volverán inestables. Si los nombres de las LUN terminan con un guión bajo y un índice entero (por ejemplo, _0 o _1), normalmente estas LUN son clones de otras LUN dentro del mismo volumen. Es posible que se monte otro backup de la base de datos o que exista un clon de otro backup. Resolución: Migre los LUN que la base de datos no usa en un volumen diferente. Si las LUN asignadas son clones, busque backups montados de la misma base de datos o clones de la base de datos, y desmonte el backup o quite el clon. No se puede anular.

Problema	Se requiere pasar	Detalles
LAS LUN sin asignar en el volumen que no forman parte del ámbito de restauración se revierten	No	Existen otras LUN distintas de las solicitadas para restaurar en el volumen. Estas LUN no están actualmente asignadas a ningún host, por lo que al restaurarse no se interrumpen los procesos activos. Sin embargo, se puede quitar la asignación de las LUN temporalmente. Solución: Migre los LUN que la base de datos no usa en un volumen diferente o elimine los LUN. Si anula esta comprobación, la restauración de volumen revertirá estas LUN al estado en que se realizó la copia Snapshot. Si la LUN no existía cuando se hizo la copia Snapshot, la LUN no existirá después de la restauración de un volumen. Anule esta comprobación solo si tiene la seguridad de que al revertir las LUN no se afectará de forma negativa en nada.
Las LUN presentes en la copia Snapshot de volumen pueden no ser coherentes al revertirse	No	Durante la creación de copias Snapshot, en el volumen existían LUN diferentes a las que se solicitó la copia Snapshot. Es posible que estas otras LUN no estén en un estado consistente. Solución: Migre los LUN que la base de datos no usa en un volumen diferente o elimine los LUN. Esto no facilita el proceso de restauración en el que falló la comprobación, pero ayudará a restaurar futuros backups creados después de mover o eliminar las LUN. Si anula esta comprobación, las LUN se revierten al estado incoherente en el que se ha hecho la copia Snapshot. Anule esta comprobación solo si tiene la seguridad de que al revertir las LUN no se afectará de forma negativa en nada.

Problema	Se requiere pasar	Detalles
Las nuevas copias Snapshot tienen un clon de volúmenes	Sí	Se han creado clones de las copias Snapshot que se crearon después de solicitar la restauración de la copia Snapshot. Dado que una restauración de volumen eliminará las copias Snapshot más adelante y no se puede eliminar una copia Snapshot si tiene un clon, no se puede realizar una restauración de volumen. Resolución: Elimine clones de copias snapshot más adelante. No se puede anular.
Se montan backups más recientes	Sí	Se montan los backups realizados después de restaurar el backup. Dado que una restauración de volúmenes elimina copias de Snapshot posteriores, no es posible eliminar una copia de Snapshot si tiene un clon, una operación de montaje de backup crea un almacenamiento clonado y no se puede ejecutar una restauración de volumen. Resolución: Desmonte la copia de seguridad posterior o restaure a partir de una copia de seguridad realizada después de la copia de seguridad montada. No se puede anular.
Existen clones de backups más recientes	Sí	Se clonan los backups realizados después de la restauración del backup. Dado que una restauración de volumen elimina copias Snapshot más adelante y no se puede eliminar una copia Snapshot si tiene un clon, no se puede realizar una restauración de volumen. Resolución: Elimine el clon del backup más nuevo o restaure desde un backup realizado después de los backups que tienen clones. No se puede anular.

Problema	Se requiere pasar	Detalles
Se pierden nuevas copias Snapshot de volumen	No	Al realizar una restauración de volumen, se eliminan todas las copias Snapshot creadas después de la copia Snapshot en la que se restaura el volumen. Si SnapManager puede asignar una copia Snapshot más adelante a un backup de SnapManager con el mismo perfil, aparecerá el mensaje "se liberarán o se eliminarán los backups más recientes". Si SnapManager no puede asignar una copia Snapshot más tarde a un backup de SnapManager en el mismo perfil, este mensaje no aparece. Solución: Restaure a partir de un backup posterior o elimine las copias snapshot más adelante. Puede anular.

Problema	Se requiere pasar	Detalles
Los backups más recientes se liberarán o se eliminarán	No	Al realizar una restauración de volúmenes, se eliminan todas las copias Snapshot creadas después de la copia Snapshot en la que se restaura el volumen. Por consiguiente, los backups creados después del backup que se va a restaurar se eliminan o se liberan. Los backups posteriores se eliminan en las siguientes situaciones: • El estado del backup no está PROTEGIDO • Retain.always FreeExpiredbackups es false en smo.config Los backups posteriores se liberan en las siguientes situaciones: • El estado del backup está PROTEGIDO • Retain.always FreeExpiredbackups es true en smo.config Resolución: Restaure a partir de una copia de seguridad posterior o libere o elimine copias de seguridad posteriores. Si anula esta comprobación, los backups creados después del backup que se está restaurando se eliminan o se liberan.

Problema	Se requiere pasar	Detalles
Se pierde la relación de SnapMirror para los volúmenes	Sí (si está deshabilitado el control de acceso basado en roles o no tiene permiso de control de acceso basado en roles)	Al restaurar un volumen en una copia Snapshot con anterioridad a la copia Snapshot de referencia en una relación de SnapMirror, se destruye la relación. Resolución: Restauración a partir de un backup creado después de la copia Snapshot básica de la relación. Como alternativa, divida la relación de almacenamiento manualmente (y luego vuelva a crear y vuelva a establecer la base de la relación una vez finalizada la restauración). Es posible anular la sustitución si el control de acceso basado en roles está habilitado y existe permiso de control de acceso basado en roles.
La relación de SnapVault para el volumen se pierde si se ha producido el proceso de restauración rápida	Sí (si está deshabilitado el control de acceso basado en roles o no tiene permiso de control de acceso basado en roles)	Al restaurar un volumen en una copia Snapshot con anterioridad a la copia Snapshot de referencia en una relación de SnapVault, se destruye la relación. Resolución: Restauración a partir de un backup creado después de la copia Snapshot básica de la relación. Como alternativa, divida la relación de almacenamiento manualmente (y luego vuelva a crear y vuelva a establecer la base de la relación una vez finalizada la restauración). No se puede reemplazar, si el control de acceso basado en roles está habilitado y tiene permiso de control de acceso basado en roles.
Se revierten los archivos NFS del volumen que no formen parte del ámbito de restauración	No	Los archivos presentes en el volumen del sistema de almacenamiento, que no son visibles en el host, se revierten si se realiza una restauración de volumen. Resolución: Migre los archivos no utilizados por la base de datos a un volumen diferente o elimine los archivos. Puede anular. Si anula este fallo de comprobación, se eliminan las LUN.

Problema	Se requiere pasar	Detalles
Los recursos compartidos de CIFS existen para el volumen	No	El volumen que se restaura tiene recursos compartidos CIFS. Es posible que otros hosts estén accediendo a los archivos del volumen durante la restauración del volumen. Resolución: Elimine los recursos compartidos CIFS innecesarios. Puede anular.
Restauración desde una ubicación alternativa	Sí	Se proporcionó una especificación de restauración para la operación de restauración que especifica que los archivos se restauren desde una ubicación alternativa. Solo se pueden utilizar las utilidades de copia del lado del host para restaurar desde una ubicación alternativa. Resolución: Ninguna. No se puede anular.
No se admite la restauración del sistema de archivos en el lado del almacenamiento en una base de datos de ASM de RAC	Sí	No se puede anular.

Recuperación de backups

En SnapManager, se deben ejecutar las operaciones de restauración y recuperación al mismo tiempo. No se puede realizar una operación de restauración y, posteriormente, se puede realizar una operación de recuperación de SnapManager.

En SnapManager 3.2 o anterior, se puede utilizar SnapManager para restaurar y recuperar la copia de seguridad o utilizar SnapManager para restaurar la copia de seguridad y utilizar otra herramienta, como Oracle Recovery Manager (RMAN), para recuperar los datos. Puesto que SnapManager puede registrar sus copias de seguridad con RMAN, puede utilizar RMAN para restaurar y recuperar la base de datos con granularidades más finas como los bloques. Esta integración combina las ventajas de la velocidad y la eficiencia del espacio de las copias Snapshot con el nivel de control preciso para la restauración mediante RMAN.

> Debe recuperar una base de datos antes de poder utilizarla. Puede utilizar cualquier herramienta o script para recuperar una base de datos.

A partir de SnapManager 3.2 para Oracle, SnapManager permite restaurar automáticamente backups de bases de datos con los backups de registros de archivos. Incluso cuando los backups de registros de archivos están disponibles en la ubicación externa, SnapManager utiliza los backups de registros de archivos desde la ubicación externa para restaurar los backups de la base de datos.

Si se agregan nuevos archivos de datos a la base de datos, Oracle recomienda realizar una nueva copia de seguridad inmediatamente. Además, si restaura una copia de seguridad realizada antes de agregar los nuevos archivos de datos e intenta recuperar a un punto después de agregar los nuevos archivos de datos, el proceso de recuperación automática de Oracle podría fallar, ya que no puede crear archivos de datos. Consulte la documentación de Oracle para conocer el proceso de recuperación de los archivos de datos agregados después de una copia de seguridad.

Estado de la base de datos necesario para el proceso de restauración

El estado de la base de datos que se va a restaurar depende del tipo de proceso de restauración que se desee realizar y del tipo de archivos que se incluirán.

En la siguiente tabla, se muestra el estado en el que la base de datos debe estar según la opción de restauración seleccionada y el tipo de archivos que se desea incluir en la restauración:

Tipo de restauración	Archivos incluidos	Estado de la base de datos para esta instancia	Estado de la base de datos para otra instancia (solo RAC)
Solo restauración	Archivos de control	Apagado	Apagado
Archivos del sistema	Montaje o apagado	Montaje o apagado	No hay archivos del sistema
Cualquier estado	Cualquier estado	Restauración y recuperación	Archivos de control
Apagado	Apagado	Archivos del sistema	Montaje
Montaje o apagado	No hay archivos del sistema	Montar o abrir	Cualquiera

El estado de la base de datos que requiere SnapManager para una operación de restauración depende del tipo de restauración que se ejecute (archivos completos, parciales o de control). SnapManager no realiza la transición de la base de datos a un estado inferior (por ejemplo, de Open a Mount) a menos que se especifique la opción force.

Qué planes de vista previa de restauración son

SnapManager ofrece planes de restauración antes y después de que se completa una operación de restauración. Los planes de restauración se utilizan para obtener una vista previa, revisar y analizar con respecto a los diferentes métodos de restauración.

Estructura del plan de restauración

El plan de restauración consta de las dos secciones siguientes:

- Vista previa/revisión: Esta sección describe cómo restaurará SnapManager cada archivo (o lo ha restaurado).
- Análisis: En esta sección se describe por qué no se utilizaron algunos mecanismos de restauración durante la operación de restauración.

La sección Vista previa/revisión

Esta sección muestra cómo se restaurará o se restaurará cada archivo. Al ver el plan de restauración antes de una operación de restauración, se denomina vista previa. Cuando se visualiza después de completar una operación de restauración, se denomina revisión.

El siguiente ejemplo de vista previa muestra que los archivos se restauran utilizando métodos rápidos basados en volúmenes, restauración del sistema de archivos en el lado del almacenamiento y restauración del sistema en el lado del almacenamiento. Para determinar por qué no se restaurarían todos los archivos utilizando el mismo método de restauración, consulte la sección Análisis.

```
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
```

Cada método de restauración tiene una subsección que contiene información sobre los archivos que se pueden restaurar mediante ese método de restauración. Las subsecciones se ordenan según niveles decrecientes de eficiencia de los métodos de almacenamiento. En el ejemplo anterior, el método de restauración rápida es más eficiente que el método de restauración del sistema de archivos de almacenamiento, y así se muestra primero.

Es posible restaurar un archivo mediante varios métodos de restauración. Se utilizan varios métodos de restauración cuando los números de unidad lógica (LUN) subyacentes utilizados en un sistema de archivos se distribuyen entre los volúmenes del sistema de almacenamiento diferentes y algunos volúmenes son aptos para la restauración de volúmenes, mientras que otros no lo son. Si se utilizan varios métodos de restauración para restaurar el mismo archivo, la sección de vista previa será similar a la siguiente:

```
The following files will be restored via a combination of:
[fast restore, storage side file system restore. storage side system
restore]
```

La sección Análisis

La sección Análisis presenta las razones por las que algunos mecanismos de restauración no se utilizarán o no. Puede usar esta información para determinar qué es necesario para habilitar mecanismos de restauración más eficientes.

En el siguiente ejemplo se muestra una sección de análisis:

```
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.
```

En el ejemplo, el primer fallo se puede anular utilizando -fast -override en la interfaz de línea de comandos (CLI) o seleccionando **Override** en la interfaz gráfica de usuario (GUI). El segundo fallo en las LUN asignadas del volumen es obligatorio y no se puede superar.

Puede resolver las comprobaciones haciendo lo siguiente:

- Para resolver un fallo de comprobación obligatorio, cambie el entorno de modo que se apruebe la comprobación.
- Para resolver un fallo de comprobación anulable, puede cambiar el entorno o anular la comprobación.

  Sin embargo, debe tener cuidado porque la anulación de la comprobación puede resultar en consecuencias no deseadas.

Previsualizar la información de restauración de copias de seguridad

Puede obtener una vista previa de la información sobre un proceso de restauración de backup antes de que se produzca para ver información sobre la idoneidad para la restauración que SnapManager para Oracle encontró en el backup. SnapManager analiza los datos del backup para determinar si el proceso de restauración puede completarse correctamente.

La vista previa de la restauración proporciona la siguiente información:

- Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se puede utilizar para restaurar cada archivo.
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo al especificar la opción -verbose.

Si especifica la opción de vista previa en el comando backup restore, SnapManager no restaura nada, sino que enumera los archivos que se van a restaurar e indica cómo se restaurarán.

> Puede obtener una vista previa de todos los tipos de mecanismos de restauración. La vista previa muestra información acerca de un máximo de 20 archivos.

1. Introduzca el siguiente comando:smo backup restore -profileprofile_name-labellabel-complete -preview -verbose

   Por ejemplo, introduzca:

   ```
   smo backup restore -profile targetdb1_prof1
         -label full_bkup_sales_nov_08  -complete -preview -verbose
   ```

   En el siguiente ejemplo, se muestran algunos archivos que se restauran con el proceso de restauración de copias de archivos del lado del host, además de explicar por qué algunos archivos no se pueden restaurar con la opción de restauración rápida. Si especifica la opción -verbose, SnapManager muestra una sección de vista previa y una sección de análisis que explica por qué no se puede restaurar cada archivo mediante el proceso de restauración rápida.

```
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. Revise los motivos por los que no pueden usarse otros procesos de restauración.
3. Inicie la operación de restauración sin la opción -preview, si sólo se muestran motivos que se pueden abreviar.

   Aún puede anular comprobaciones no obligatorias.

Restauración de backups mediante restauración rápida

Si se cumplen todas las condiciones obligatorias de restauración rápida, es posible forzar a SnapManager para Oracle que utilice el proceso de SnapRestore basado en

volúmenes en lugar de otros procesos de restauración.

Se puede utilizar el comando backup restore con -fast: `backup restore -fast [require | override | fallback | off]`

La opción -FAST solo se puede utilizar si se desea realizar una restauración completa de un backup completo. La opción -fast incluye los siguientes parámetros:

- Requerir: Le permite realizar una restauración de volúmenes si se cumplen todas las condiciones de elegibilidad de restauración obligatorias y no se encuentran comprobaciones que puedan realizarse.

  Si se especifica la opción -fast, pero no se especifica ningún parámetro para -FAST, SnapManager utiliza el parámetro-require como valor predeterminado.

- Anular: Permite anular las comprobaciones de elegibilidad no obligatorias y realizar la restauración rápida basada en volumen.
- Fallback: Permite restaurar la base de datos con el método que SnapManager determina.

  Si no se especifica -fast, SnapManager utiliza el parámetro -fallback como valor predeterminado.

- Desactivado: Permite evitar el tiempo necesario para realizar todas las comprobaciones de elegibilidad, para realizar un proceso de restauración basado en archivos en lugar del proceso de restauración rápido.

Si la copia de seguridad no supera las comprobaciones de elegibilidad obligatorias, la restauración rápida no se puede completar correctamente.

SnapManager realiza restauraciones rápidas basadas en volúmenes únicamente en entornos basados en UNIX; SnapManager no realiza restauraciones rápidas en el entorno Windows.

Al realizar VBSR en la copia de seguridad del archivo de datos, si los archivos de datos y los archivos de registro de archivos están presentes en el mismo volumen y si los archivos de registro de archivos no están presentes en el sistema de archivos activo, la restauración y recuperación de la base de datos se realiza correctamente. Sin embargo, las futuras snapshots de registros de archivos se eliminan como parte de VBSR. Esto provoca una entrada obsoleta del backup de registros de archivos en el repositorio.

1. Introduzca el siguiente comando:SMO backup restore -profileprofile_name-labellabel-complete-fast require-verbose

   ```
   smo backup restore -profile targetdb1_prof1
         -label full_bkup_sales_nov_08  -complete -fast require -verbose
   ```

2. Revisar las comprobaciones de cumplimiento de la restauración rápida.
3. Si la comprobación de elegibilidad determina que no se ha producido un error en las comprobaciones obligatorias, si se pueden anular ciertas condiciones y si desea continuar con el proceso de restauración, escriba el siguiente comando: Backup restore -fast override

Información relacionada

Crear scripts de tareas previas, tareas posteriores y directivas

Variables disponibles en los scripts de tareas para la operación de restauración

Restauración de backups mediante Single File SnapRestore

Para restaurar los backups, se puede utilizar el método Single File SnapRestore (SFSR).

1. Cree un perfil desde la interfaz gráfica de usuario (GUI) de SnapManager.
2. Realice una copia de seguridad de la base de datos mediante la GUI.
3. Desenlazar los grupos de servicios de Oracle y Network File System (NFS) de los grupos de servicios de cluster y congelarlos.
4. Asegúrese de que Secure Shell (SSH) esté configurado entre los hosts y SnapDrive para UNIX estableciendo #Secure-comunic-in-cluster-nodes en el archivo snapdrive.conf.
5. Desde la interfaz gráfica de usuario de SnapManager, puede realizar una restauración y recuperación de backup completa mediante --alllogs.
6. Descongele los grupos de servicios y vincúlelos al grupo de servicios del clúster.

> Esta configuración sólo se aplica cuando se utiliza SnapDrive 4.1.1 D2 para UNIX y SnapDrive 4.2 para UNIX.

Si una operación de restauración es seguida de otra, existe la posibilidad de que se produzca un error en la creación de la copia de Snapshot de backup. Si se ejecutan operaciones de restauración sucesivas en el periodo especificado en el que se puede completar SFSR, SnapManager para Oracle encontrará errores de creación de copias Snapshot.

Para evitar errores de creación de copias de Snapshot, asegúrese de que se realicen operaciones de restauración después del periodo durante el cual se SFSR en curso.

Para ello, compruebe el estado del proceso de división de clones de la LUN introduciendo el siguiente comando desde la interfaz de línea de comandos (CLI) del sistema de almacenamiento: Rshfilernnamelun clone sparruslun-name

```
Sample Output:
/vol/delaware_760gb/lun700gb (64% complete)..
```

> El SnapRestore basado en volúmenes (VBSR) no es compatible con los hosts Solaris que ejecutan Veritas stack con entornos SFRAC y VCS.

Restaurar backups en el almacenamiento principal

Es posible utilizar el comando backup restore para restaurar un backup de base de datos en el almacenamiento primario.

SnapManager intenta realizar una restauración rápida basada en volúmenes de forma predeterminada y proporciona información de comprobación de elegibilidad. Si es necesario, puede anular algunas comprobaciones de elegibilidad. Si está seguro de que no se puede realizar una copia de seguridad mediante una restauración rápida, puede deshabilitar la verificación de elegibilidad rápida para la restauración y realizar una restauración basada en archivos.

Es posible usar las opciones del comando backup restore para especificar si SnapManager debe restaurar todo el backup o parte de él. SnapManager también permite restaurar archivos de control junto con los archivos de datos o los espacios de tablas desde los backups en una sola operación de usuario. Se pueden incluir -controlfiles con -complete para restaurar archivos de control, junto con espacios de tablas y archivos de datos.

Se pueden seleccionar una de las siguientes opciones para restaurar el backup:

Si desea restaurar…	Usar…
Todo el backup con todos los espacios de tablas y ficheros de datos	-completo
Lista de tablespaces específicos	-tablespaces
Archivos de datos específicos	-archivos
Solo los archivos de control	-controlfiles
Espacios de tabla, archivos de datos y archivos de control	-complete -controlfiles

También puede restaurar el backup desde una ubicación alternativa especificando -restoreespec.

Si incluye -recover, puede recuperar la base de datos en:

- La última transacción que se produjo en la base de datos (todos los registros)
- Una fecha y hora específicas
- Un número de cambio de sistema (SCN) específico
- La hora del backup (sin registros)
- Solo restauración

> Tanto la recuperación de fecha y hora como la recuperación de SCN son recuperaciones puntuales.

SnapManager (3.2 o posterior) permite recuperar los backups de la base de datos restaurada automáticamente mediante los archivos de registro de archivos. Aunque los archivos de registro de archivos estén disponibles en la ubicación externa, si se especifica la opción -recover-from-location, SnapManager utiliza los archivos de registro de archivos de la ubicación externa para recuperar los backups de la base de datos restaurada.

SnapManager proporciona la ubicación externa a Oracle. Sin embargo, Oracle no identifica los archivos desde el destino externo. Este comportamiento se observa en los destinos de área de recuperación de flashy en el destino de gestión automática de almacenamiento (ASM). Se trata de problemas con Oracle y la solución alternativa es tener siempre una copia de seguridad de los archivos de registro de archivos en dichos diseños de bases de datos.

Si se proporciona un SCN o fecha incoherentes, la recuperación se detendrá en el último punto consistente recuperado con el mensaje de error recuperación correcta, pero insuficiente. Es necesario realizar manualmente la recuperación a un estado consistente.

Para la recuperación cuando no se aplican registros, SnapManager se recupera hasta el último SCN del último archivo de registro de archivos creado durante el backup. Si la base de datos es coherente hasta este SCN, la base de datos se abrirá correctamente. Si la base de datos no es coherente en este momento, SnapManager sigue intentando abrir la base de datos, que se abrirá correctamente si la base de datos ya es coherente.

> SnapManager no admite la recuperación de los backups de solo registro de archivos.

Si la separación de registros de archivosen un punto de montaje NFS no es un almacenamiento compatible con Snapshot, SnapManager permite recuperar los backups de la base de datos restaurada mediante el perfil. Antes de ejecutar operaciones de SnapManager en un almacenamiento que no es compatible con Snapshot, debe añadir los destinos para archivedLogs.Exclude en smo.config.

Debe asegurarse de establecer el parámetro Exclude antes de crear un perfil. Sólo después de establecer el parámetro exclude en el archivo de configuración de SnapManager, la creación de perfiles se realiza correctamente.

> Si la base de datos es un almacenamiento compatible con Snapshot en un grupo de discos ASM y cuando la base de datos se selecciona como destino de registros de archivo, SnapManager no admite la restauración de los backups con el perfil.

Si el backup ya está montado, SnapManager no monta el backup de nuevo y utiliza el backup ya montado. Si la copia de seguridad está montada por un usuario diferente y si el usuario actual no tiene acceso a la copia de seguridad previamente montada, otros usuarios tienen que proporcionar los permisos. Todos los archivos de registro de archivos tienen permisos de lectura para los propietarios de los grupos; es posible que el usuario actual no obtenga los permisos, si el backup está montado por otro grupo de usuarios. Los usuarios pueden proporcionar permisos a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la restauración o recuperación.

Recuperar backups de una base de datos en un entorno RAC

Durante la recuperación de los backups de la base de datos en un entorno RAC, cuando no se encuentra el archivo de registro de archivo necesario, Oracle solicita archivos de registro de archivo y cambia entre diferentes subprocesos y número de cambio en la base de datos RAC. SnapManager para Oracle intenta recuperar la base de datos como mejor esfuerzo. La recuperación correcta de los backups de base de datos en el entorno RAC depende de la disponibilidad de los archivos de registro de archivos en los backups.

El mecanismo de recuperación recomendado para la base de datos RAC es el siguiente:

- Asegúrese de que todos los archivos de registro de archivos estén disponibles en los backups o que todos los archivos de registro de archivos estén disponibles en el único destino de registro de archivos externo.
- Si se proporcionan varios destinos de registros de archivos externos, puede proporcionar solapamiento de los archivos de registro de archivos al tiempo que especifica los destinos de registros de archivos externos para todos los subprocesos.

  Por ejemplo, la ubicación del archivo de registro externo: Puedo tener entre 1 y 100 archivos de registro de archivo, la ubicación del archivo de registro externo - II puede tener entre 98 y 200 archivos de registro de archivo y la ubicación del archivo de registro externo - III puede tener entre 198 y 300 archivos de registro de archivo.

- Al eliminar los archivos de registro de archivos, en lugar de eliminar todos los archivos de registro de archivos, es posible eliminar los archivos de registro de archivos hasta SCN o fecha para que los backups puedan tener los mismos archivos de registro de archivos.

Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de restauración correcta o con errores.

1. Introduzca el siguiente comando: smo backup restore -profile profile_name-label label-complete-recover -alllogs [-recover-from-locationpath [,path2]]-dump-verbose

   smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 - complete -recover -alllogs -verbose

2. Para restaurar datos en diferentes situaciones, complete una de las siguientes acciones:

Si desea restaurar…	Ejemplo de comando
Complete Database sin archivos de control y recupere un número SCN en particular (3794392). En este caso, existen los archivos de control actuales, pero todos los archivos de datos están dañados o perdidos. Restaure y recupere la base de datos de una copia de seguridad en línea completa existente a un punto inmediatamente anterior a ese SCN.	smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -until 3794392 -verbose
Completar la base de datos sin archivos de control y recuperar hasta una fecha y hora.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -until 2008-09-15:15:29:23 -verbose
Completar la base de datos sin archivos de control y recuperar hasta datos y tiempo. En este caso, existen los archivos de control actuales, pero todos los archivos de datos están dañados o se pierden o se produjo un error lógico después de un momento específico. Restaure y recupere la base de datos de una copia de seguridad en línea completa existente a una fecha y hora inmediatamente antes del punto de fallo.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -until "2008-09-15:15:29:23" -verbose
Base de datos parcial (uno o más archivos de datos) sin archivos de control y recuperación mediante todos los registros disponibles. En este caso, existen los archivos de control actuales, pero uno o más archivos de datos están dañados o perdidos. Restaure esos archivos de datos y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	restauración de copia de seguridad de smo -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -files /u02/oradata/ventes02.dbf /u02/oradata/ventes03.dbf /u02/oradata/ventes.04.dbf -recover -alllogs -verbose

Si desea restaurar…	Ejemplo de comando
Base de datos parcial (uno o más tablespaces) sin archivos de control y recuperación mediante todos los registros disponibles. En este caso, existen los archivos de control actuales, pero se pierden uno o más tablespaces o se pierde uno de los más archivos de datos pertenecientes al tablespace. Restaure esos tablespaces y recupere la base de datos a partir de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -tablespaces users -recover -alllogs -verbose
Sólo archivos de control y recuperación mediante todos los registros disponibles. En este caso, los archivos de datos existen, pero todos los archivos de control están dañados o perdidos. Restaure sólo los archivos de control y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -controlfiles -recover -alllogs -verbose
Complete la base de datos sin archivos de control y recupérese usando los archivos de control de copia de seguridad y todos los registros disponibles. En este caso, todos los archivos de datos están dañados o perdidos. Restaure sólo los archivos de control y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -using-backup -controulfile -recover -alllogs -verbose
Recupere la base de datos restaurada utilizando los archivos archive log de la ubicación externa del archive log.	smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -using-backup -controulfile -recover -alllogs -recover-from-location /user1/archive -verbose

3. Revisar las comprobaciones de cumplimiento de la restauración rápida.

   Introduzca el siguiente comando: smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -alllogs -recover-from-location /user1/archive -verbose

4. Si la comprobación de elegibilidad muestra que no se ha producido un error en las comprobaciones obligatorias y si se pueden anular ciertas condiciones y si desea continuar con el proceso de restauración, escriba lo siguiente: Restauración de copia de seguridad - anulación rápida
5. Especifique las ubicaciones de los registros de archivos externos con la opción -recover-from-location.

Información relacionada

Restauración de backups mediante restauración rápida

Restaurar backups desde una ubicación alternativa

El comando smo backup restore

Realizar recuperaciones a nivel de bloque con Oracle Recovery Manager (RMAN)

Puede configurar SnapManager para catalogar sus backups en Recovery Manager (RMAN), una herramienta de Oracle, de modo que pueda realizar una recuperación a nivel de bloque con RMAN. RMAN puede utilizar los archivos de control de la base de datos o una base de datos de catálogo de recuperación independiente como repositorio.

1. Para realizar un backup completo sin conexión mediante SnapManager, introduzca el siguiente comando:

   el backup de smo crea -offline-full-profeprofile_name-labelbackup_label_name-verbose

   Donde:

   - profile_name es el nombre del perfil asociado a la copia de seguridad
   - backup_label_name es el nombre de la etiqueta de backup

```
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. Para verificar que el backup está catalogado con RMAN, en el host de la base de datos, introduzca el siguiente comando en el símbolo del sistema de RMAN:

   listar etiqueta de datafilocopia 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. Para verificar la base de datos y determinar si algún bloque está dañado, introduzca el siguiente comando:

   dbv FILE=user01.dbf

   La siguiente salida muestra que dos páginas están dañadas:

```
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. Para que los archivos de la copia de seguridad sean accesibles en el host y en RMAN, monte la copia de seguridad con el siguiente comando:

   montaje de backup de smo -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. Para recuperar los bloques, en RMAN, introduzca el siguiente comando:

   blockrecover file "/mountpoint/path/file.dbf" block_id, from 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. Para verificar si los bloques se han reparado, utilice el siguiente comando:

   dbv FILE=filename.dbf

   La siguiente salida muestra que ninguna página está dañada:

```
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)
```

   Todos los bloques dañados fueron reparados y restaurados.

Restaurar los archivos de una ubicación alternativa

SnapManager le permite restaurar archivos de datos y archivos de control desde una

ubicación distinta a la de las copias Snapshot del volumen original.

La ubicación original es la ubicación del archivo en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es la ubicación desde la cual se restaurará un archivo.

Puede restaurar los siguientes datos desde una ubicación alternativa:

- Los archivos de datos de un sistema de archivos intermedio a un sistema de archivos activo
- Bloques de datos de un dispositivo RAW intermedio en un dispositivo RAW activo

SnapManager automatiza la recuperación. Al recuperar archivos de ubicaciones externas, SnapManager utiliza el comando recovery automatic from location.

SnapManager también usa Oracle Recovery Manager (RMAN) para recuperar archivos. Oracle debe reconocer los archivos que se van a recuperar. Los nombres de archivo deben tener el formato predeterminado. Al recuperarse del área de recuperación de flash, SnapManager ofrece la ruta traducida a Oracle. Sin embargo, Oracle no se recupera del área de recuperación de flash porque no puede generar el nombre de archivo correcto. Lo ideal es que el área de recuperación de flash sea un destino diseñado para trabajar con RMAN.

Información relacionada

Creando especificaciones de restauración

Restaurar backups desde una ubicación alternativa

Para restaurar una copia de seguridad de la base de datos desde una ubicación alternativa, utilice los siguientes pasos principales, cada uno de los cuales se describe más adelante en esta sección.

- Realice una de las siguientes acciones, según la distribución de la base de datos y qué debe restaurarse:
  - Restaurar los archivos de datos necesarios desde cinta, SnapVault, SnapMirror o cualquier otro medio en cualquier sistema de archivos montado en el host de la base de datos.
  - Restaurar el sistema de archivos requerido y montarlo en el host de la base de datos.
  - Conéctese a los dispositivos RAW necesarios que existen en el host local.
- Cree un archivo XML (Lenguaje de marcado extensible) de especificación de restauración que incluya las asignaciones que SnapManager necesita para restaurar desde la ubicación alternativa a la ubicación original. Guarde el archivo en una ubicación a la que SnapManager pueda acceder.
- Utilice SnapManager para restaurar y recuperar los datos con el archivo XML de especificación de restauración.

Restauración de los datos de los archivos

Antes de restaurar desde una ubicación alternativa, debe restaurar los archivos necesarios desde cualquier medio de almacenamiento y restaurar los archivos de aplicaciones como SnapVault o SnapMirror a un sistema de archivos montado en el host local.

Es posible utilizar la restauración desde una operación de ubicación alternativa para copiar los archivos de un sistema de archivos alternativo a un sistema de archivos activo.

Debe especificar las ubicaciones alternativas desde las que desea restaurar los archivos originales mediante la creación de una especificación de restauración.

Restauración de datos desde el sistema de ficheros

Antes de restaurar datos desde una ubicación alternativa, debe restaurar el sistema de archivos necesario y montarlo en el host local.

Se puede invocar la operación de restauración desde una ubicación alternativa para copiar los archivos de sistemas de archivos alternativos a sistemas de archivos activos.

Para realizar esta operación, debe especificar los puntos de montaje alternativos desde los que se restaurarán los puntos de montaje originales y los nombres de las copias Snapshot originales creando un archivo de especificación de restauración.

> El nombre de copia Snapshot es un componente necesario porque el mismo sistema de archivos puede ajustarse varias veces en una única operación de backup (por ejemplo, una vez para los archivos de datos y otra para el archivo de registro).

Para Automatic Storage Management (ASM), el nombre del grupo de discos debe ser el mismo que el grupo de discos clonado por SnapManager para registrar la copia de seguridad con Oracle Recovery Manager (RMAN). Para obtener este nombre, consulte las propiedades de la copia de seguridad.

Información relacionada

Creando especificaciones de restauración

Restauración de los datos desde dispositivos sin configurar

Antes de restaurar desde una ubicación alternativa, debe conectarse a los dispositivos sin formato necesarios que existan en el host local.

Puede invocar la restauración desde una operación de ubicación alternativa para copiar los bloques de datos de dispositivos sin formato alternativos a dispositivos sin formato activos. Para realizar esta operación, debe especificar el dispositivo RAW alternativo desde el que restaurar el dispositivo RAW original creando una especificación de restauración.

Información relacionada

Creando especificaciones de restauración

Creando especificaciones de restauración

El archivo de especificación de restauración es un archivo XML que contiene las ubicaciones originales y alternativas desde las que se puede restaurar el archivo. SnapManager utiliza este archivo de especificación para restaurar los archivos desde la ubicación especificada.

Puede crear el archivo de especificación de restauración usando cualquier editor de texto. Se debe usar la extensión .xml del archivo.

1. Abra un archivo de texto.

2. Introduzca lo siguiente: <restore-specification xmlns="" class="bare">http://www.netapp.com">
3. Introduzca cualquier información de asignación de archivos con el formato que se muestra en el ejemplo siguiente:

```
<file-mapping>
    <original-location>/path/dbfilename.dbf</original-location>
    <alternate-location>/path/dbfilename1.dbf</alternate-location>
</file-mapping>
```

La asignación de archivos especifica desde dónde se restaura un archivo. La ubicación original es la ubicación del archivo en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es la ubicación desde la que se restaura el archivo.

4. Introduzca cualquier información de asignación del sistema de archivos montado con el formato que se muestra en el ejemplo:

```
<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>
```

Mountpoint hace referencia a la ruta de directorio /mnt/myfs/)o a un punto de montaje de grupo de discos de Automatic Storage Management (ASM) (por ejemplo, +MY_DG). La asignación de punto de montaje especifica el punto de montaje desde el que se restauran los archivos. La ubicación original es la ubicación del punto de montaje en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es el punto de montaje desde el que se restauran los archivos de la ubicación original. Snapname es el nombre de la copia Snapshot en la que se realizó el backup de los archivos originales.

Para ASM, el nombre del grupo de discos debe ser el mismo que el grupo de discos clonado de SnapManager para registrar el backup con RMAN. Para obtener este nombre, consulte las propiedades de la copia de seguridad.

> El nombre de copia Snapshot es un componente necesario porque el mismo sistema de archivos se puede usar varias veces en una única operación de backup (por ejemplo, una vez para los archivos de datos y una vez para los registros).

5. Introduzca las etiquetas y ubicaciones de asignación de dispositivos sin procesar con el formato que se muestra en el ejemplo:

```
<raw-device-mapping>
     <original-location>/path/raw_device_name</original-location>
     <alternate-location>/path/raw_device_name</alternate-location>
</raw-device-mapping>
```

La asignación de dispositivos sin formato especifica la ubicación desde la que se restaura un dispositivo sin formato.

6. Introduzca lo siguiente: </restore-specification>
7. Guarde el archivo como un archivo .xml y cierre la especificación.

Restaurar ejemplo de especificación

En el ejemplo siguiente se muestra la estructura de especificación de restauración:

```
<?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>
```

Restaurar backups desde una ubicación alternativa

Es posible restaurar backups desde una ubicación alternativa para restaurar los archivos

de datos desde un sistema de archivos intermedio a un sistema de archivos activo, o bien restaurar los bloques de datos desde un dispositivo sin formato intermedio en un dispositivo sin formato activo.

- Cree un archivo XML de especificación de restauración y especifique el tipo de método de restauración que desea utilizar.

Es posible usar el comando smo backup restore y especificar el archivo XML de especificación de restauración que se creó para restaurar el backup desde una ubicación alternativa.

1. Escriba el siguiente comando: smo backup restore -profileprofile-labellabel-complete-alllogs -restorespecirestoreespec

Información relacionada

El comando smo backup restore

Clonar el backup de bases de datos

Si clona una base de datos, puede realizar tareas como probar una actualización a una base de datos sin afectar a la base de datos en producción, duplicar una instalación maestra a varios sistemas de entrenamiento o duplicar una instalación maestra como instalación básica a otros servidores, que tienen requisitos similares.

Puede ejecutar las siguientes tareas relacionadas con la clonado:

- Clonar una base de datos a partir de un backup existente.
- Clonar una base de datos en su estado actual, lo que permite crear el backup y el clon en un procedimiento.
- Clone un backup protegido en el almacenamiento secundario o incluso terciario.
- Clone una base de datos y utilice scripts de plugins personalizados, que se ejecutan antes o después de la operación de clonado.
- Clone una base de datos en el mismo host en el que reside la base de datos.
- Clone una base de datos con los archivos de registro de archivos desde la ubicación del registro de archivos externo.
- Clonar una base de datos en un host alternativo.
- Clonar una base de datos RAC.
- Consulte una lista de clones.
- Ver información detallada sobre clones.
- Eliminar clones.

Qué es la clonación

Puede clonar una base de datos para crear una réplica exacta de la base de datos original. Es posible crear el clon a partir de un backup completo o desde el estado actual de la base de datos.

A continuación se presentan algunas de las ventajas de crear un clon con SnapManager:

Ventajas	Detalles
Velocidad	La operación de clonación de SnapManager usa la función FlexClone disponible con Data ONTAP. Esto permite clonar rápidamente grandes volúmenes de datos.
Gestión eficiente del espacio	Cuando crea un clon con SnapManager, solo se necesita espacio para los cambios entre el backup y el clon. Un clon SnapManager es una copia Snapshot editable de la base de datos original y puede crecer según sea necesario. Por el contrario, un clon físico de la base de datos requiere que disponga de espacio suficiente para copiar la base de datos completa.
Copia virtual	Puede utilizar la base de datos clonada como si fuera la base de datos original. Por ejemplo, puede usar un clon para pruebas, comprobaciones de plataformas y actualizaciones, simulaciones múltiples aplicadas a un conjunto de datos de gran tamaño, y pruebas y almacenamiento provisional en oficinas remotas. Los cambios en el clon no afectan a la base de datos original. Una vez clonada la base, la base de datos clonada queda totalmente operativa.
Sencillez	Es posible clonar una base de datos a cualquier host con los comandos de SnapManager.

Es posible clonar un backup en el almacenamiento primario (local) o un backup protegido que está en el almacenamiento secundario (remoto). Sin embargo, no es posible clonar un backup si la operación de backup está en curso o si el backup se transfirió al almacenamiento secundario.

Para poder clonar una base de datos, debe asegurarse de que se cumplen los siguientes requisitos previos:

- Asegúrese de que el directorio [/etc|/var/opt/oracle]/oratab no contenga una entrada que apunte al identificador del sistema de destino.
- Elimine el archivo speLATRY <SID>.ora de $ORACLE_HOME/DBS.
- Elimine el archivo <SID>.ora de $ORACLE_HOME/DBS.
- Elimine los destinos de volcado de Oracle que estén especificados en el archivo de especificación del clon.
- Elimine los archivos de control de Oracle que estén especificados en el archivo de especificación del clon.
- Elimine los archivos de registro de recuperación de Oracle especificados en el archivo de especificación del clon.

Debe proporcionar al clon un nuevo identificador del sistema. No se pueden ejecutar simultáneamente dos bases de datos con el mismo identificador de sistema en el mismo host. Es posible tener un clon en otro host con el mismo identificador de sistema. Es posible asignar al clon una etiqueta o dejar que SnapManager cree

una etiqueta con el identificador del sistema, la fecha y la hora en que se creó el clon.

Cuando introduce una etiqueta, no debe incluir espacios ni caracteres especiales.

Como parte del proceso de clonado, SnapManager crea los parámetros y archivos de Oracle necesarios para la base de datos clonada. Un ejemplo de un archivo de Oracle necesario es el archivo <SID>.ora de Re.

Cuando se clona una base de datos, SnapManager crea un nuevo archivo <SID>.ora para la base de datos en el directorio $ORACLE_HOME/DBS.

Cuando SnapManager clona el almacenamiento de una base de datos, también crea un nuevo punto de montaje del sistema de archivos, pero no cambia la estructura de directorio en el punto de montaje desde la CLI de SnapManager. No obstante, desde la interfaz gráfica de usuario de SnapManager, es posible cambiar la estructura de directorio y los metadatos del sistema de archivos.

Oracle 11g en un entorno de NFS directo (DNFS) permite una configuración de punto de montaje adicional, como varias rutas para el equilibrio de carga en el archivo Naranfstab. SnapManager no modifica este archivo, por lo que cualquier propiedad adicional que desee que utilice un clon debe agregarse manualmente al archivo oranfstab después de realizar la clonación con SnapManager.

Puede clonar una base de datos de Real Application Cluster (RAC) y una base de datos no cluster. Un clon de RAC se inicia como una sola base de datos.

Es posible clonar un backup de base de datos en el host en el que reside la base de datos o en un host alternativo.

También es posible clonar una base de datos ASM en un host remoto. Cuando lo haga, debe asegurarse de que la instancia de ASM esté en ejecución en el host remoto.

Si la base de datos clonada utilizaba un archivo spfile, SnapManager crea un archivo spfile para el clon. Coloca este archivo en el directorio $ORACLE_HOME/DBS y crea la estructura de directorios para los archivos de diagnóstico. el nombre de archivo es spfile <SID>.ora.

Métodos de clonación

Es posible clonar una base de datos mediante uno de estos dos métodos. El método seleccionado afecta a la operación de creación de clon.

En la siguiente tabla se describen los métodos de clonado y su efecto en la operación clone create y su opción -reserve. Una LUN se puede clonar mediante cualquiera de los dos métodos.

Método de clonación	
Descripción	
clone create -reserve	
Clonado de LUN	
Se crea un nuevo LUN clon en el mismo volumen.	
Cuando -reserve para una LUN está establecida en yes, se reserva espacio para todo el tamaño de LUN dentro del volumen.	

Método de clonación
Clonado de volúmenes
Se crea un nuevo FlexClone y la LUN clonada existe dentro del nuevo volumen clonado. Utiliza la tecnología FlexClone.
Cuando -reserve para un volumen está establecida en yes, se reserva espacio para todo el tamaño del volumen dentro del agregado.

Creando especificaciones de clon

SnapManager para Oracle utiliza un archivo XML de especificación del clon, que incluye las asignaciones, las opciones y los parámetros que se deben utilizar en la operación de clonado. SnapManager utiliza esta información para determinar dónde colocar los archivos que clona y cómo tratar información de diagnóstico, archivos de control, parámetros, etc.

Es posible crear el archivo de especificación del clon con la interfaz gráfica de usuario (GUI) de SnapManager, la interfaz de línea de comandos (CLI) o un editor de texto.

Cuando crea el archivo de especificación del clon con un editor de texto, debe guardarlo como archivo .xml. Es posible usar este archivo XML para otras operaciones de clonado.

También puede crear una plantilla de especificación de clon y personalizarla. Puede usar el comando de plantilla de clon de smo o la interfaz gráfica de usuario; use el asistente Clone.

SnapManager para Oracle agrega una cadena de versión a cualquier plantilla de especificación de clon que genere. SnapManager para Oracle asume la versión más reciente de cualquier archivo de especificación del clon que no tenga una cadena de versión.

Si desea realizar la clonado remota, no cambie las ubicaciones predeterminadas de los archivos de datos, los archivos de registro de recuperación y los archivos de control en el archivo de especificación del clon. Si cambia la ubicación predeterminada, SnapManager no puede crear el clon o crear el clon en una base de datos que no es compatible con la funcionalidad de Snapshot. Por lo tanto, la creación automática de perfil falla.

> Aunque la información del punto de montaje y del grupo de discos de ASM se puede editar desde la interfaz gráfica de usuario, solo se puede cambiar el nombre del archivo y no las ubicaciones del archivo.

Puede ejecutar una tarea varias veces, ya sea con combinaciones de parámetros y valores iguales o diferentes.

1. Abra un archivo de texto e introduzca texto como se muestra en el ejemplo siguiente:

```
<clone-specification xmlns="http://www.example.com>
     <storage-specification/>
     <database-specification/>
 </clone-specification>
```

2. En el componente de especificación de almacenamiento, introduzca los puntos de montaje para los archivos de datos.

   La especificación de almacenamiento enumera las ubicaciones para el nuevo almacenamiento creado para el clon, como puntos de montaje de archivos de datos y dispositivos sin formato. Estos elementos se deben asignar del origen al destino.

   En el ejemplo siguiente se muestra la sintaxis de punto de montaje del archivo de datos que se utiliza en la especificación del clon:

```
<mountpoint>
     <source>/mnt/path/source_data file_mountpoint</source>
     <destination>/mnt/path/target_data file_mountpoint</destination>
</mountpoint>
```

3. Opcional: Si tiene un dispositivo sin formato en el origen, debe especificar la ruta del dispositivo sin formato en el origen y, a continuación, especificar el destino auto-generate='"true" para el destino.

   A diferencia del archivo de asignación de clones de las versiones anteriores de SnapManager para Oracle, no se puede especificar una ubicación para el dispositivo sin configurar en el destino. SnapManager para Oracle elegirá el siguiente nombre de dispositivo disponible para el dispositivo RAW clonado.

   En el ejemplo siguiente se muestra la sintaxis de dispositivo sin configurar que se utiliza en la especificación del clon:

```
<raw-device>
     <source>/dev/raw/raw1</source>
     <destination auto-generate="true"/>
</raw-device>
```

4. En el componente de especificación de la base de datos, identifique la información del archivo de control como una lista de los archivos de control que desea crear para el clon.

   La especificación de la base de datos especifica las opciones de la base de datos para el clon, como los archivos de control, los registros de recuperación, los registros de archivos y los parámetros de Oracle.

   En el ejemplo siguiente se muestra la sintaxis del archivo de control que se utiliza en la especificación del clon:

```
<controlfiles>
     <file>/mnt/path/clonename/control/control01.ctl</file>
     <file>/mnt/path/clonename/control/control02.ctl</file>
</controlfiles>
```

5. Especifique la estructura del registro de recuperación para el clon.

   En el ejemplo siguiente se muestra la estructura de directorio redo log para la clonado:

```
<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. Especifique los parámetros de Oracle que deben establecerse con diferentes valores en la base de datos clonada. Si utiliza Oracle 10, debe especificar los siguientes parámetros:
   - Volcado en segundo plano
   - Volcado de memoria
   - Volcado de usuario
   - (Opcional) registros de archivo

   > Si los valores de los parámetros no están configurados correctamente, la operación de clonado se detiene y se recibe un mensaje de error.

   Si no especifica la ubicación donde se almacenan los registros de archivos, SnapManager crea el clon en modo noarchivelog. SnapManager copia esta información de parámetro en el archivo init.ora del clon.

   + en el ejemplo siguiente se muestra la sintaxis de parámetros que se utiliza en la especificación del clon:

```
<parameters>
     <parameter>
          <name>log_archive_dest_1</name>
          <value>LOCATION=/mnt/path/clonename/archive</value>
     </parameter>
</parameters>
```

+ + puede utilizar un valor predeterminado utilizando un elemento default dentro del elemento Parameter. En el ejemplo siguiente, el parámetro os_Authentication_PREFIX tomará el valor predeterminado porque se especifica el elemento predeterminado:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <default></default>
     </parameter>
</parameters>
```

+ + puede especificar una cadena vacía como valor de un parámetro mediante un elemento vacío. En el ejemplo siguiente, os_Authentication_PREFIX se establecerá en una cadena vacía:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <value></value>
     </parameter>
</parameters>
```

+ + NOTA: Puede utilizar el valor del archivo init.ora de la base de datos de origen para el parámetro sin especificar ningún elemento.

+ + Si un parámetro tiene varios valores, puede proporcionar los valores de los parámetros separados por comas. Por ejemplo, si desea mover los archivos de datos de una ubicación a otra, puede utilizar el parámetro dB_file_name_convert y especificar las rutas de acceso del archivo de datos separadas por comas, como se muestra en el ejemplo siguiente:

+

+

+

```
<parameters>
     <parameter>
          <name>db_file_name_convert</name>
          <value>>/mnt/path/clonename/data file1,/mnt/path/clonename/data
file2</value>
     </parameter>
</parameters>
```

+ + Si desea mover los archivos de registro de una ubicación a otra, a continuación puede utilizar el parámetro log_file_name_convert y especificar las rutas de acceso del archivo de registro separadas por comas, como se muestra en el ejemplo:

+

+

+

```
<parameters>
     <parameter>
          <name>log_file_name_convert</name>

<value>>/mnt/path/clonename/archivle1,/mnt/path/clonename/archivle2</value
>
     </parameter>
</parameters>
```

1. Opcional: Especifique sentencias SQL arbitrarias para que se ejecuten en el clon cuando está en línea.

   Puede utilizar las sentencias SQL para realizar tareas como la recreación de los archivos temporales en la base de datos clonada.

   > Debe asegurarse de que no se incluya un punto y coma al final de la instrucción SQL.

   A continuación se muestra una sentencia SQL de muestra que se ejecuta como parte de la operación de clonado:

```
<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>
```

Ejemplo de especificación del clon

En el ejemplo siguiente se muestra la estructura de especificaciones del clon, incluidos los componentes de especificación de base de datos y almacenamiento:

```
<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>
```

Información relacionada

Clonar bases de datos y usar scripts de plugins personalizados

Clonar bases de datos a partir de backups

Clonado de bases de datos en estado actual

Consideraciones para clonar una base de datos en un host alternativo

Clonar bases de datos y usar scripts de plugins personalizados

SnapManager proporciona un método para usar scripts personalizados antes y después de que se produzca una operación de clonado. Por ejemplo, podría haber creado un script personalizado que valida un SID de base de datos de clon y garantiza que el SID lo permita la política de nomenclatura. Mediante el plugin de clonado de SnapManager, puede incluir scripts personalizados y hacerlos ejecutar automáticamente antes o después de una operación de clonado de SnapManager.

1. Ver scripts de plugins de muestra.
2. Cree una secuencia de comandos desde cero o modifique una de las secuencias de comandos del plug-in de ejemplo.

Cree su script personalizado de acuerdo con las directrices de script del plugin de SnapManager.

3. Coloque la secuencia de comandos personalizada en una ubicación de directorio especificada.
4. Actualice el archivo XML de especificación del clon e incluya información sobre el script personalizado que debe utilizarse durante el proceso de clonado.
5. Mediante un comando de SnapManager, compruebe que los scripts personalizados estén operativos.
6. Cuando inicia la operación de clonado, incluya el nombre de script y los parámetros opcionales.

Clonar bases de datos a partir de backups

Es posible clonar una base de datos a partir de un backup con el comando clone create.

Primero debe crear un archivo de especificación del clon para la base de datos. SnapManager crea el clon según la información de este archivo de especificación.

Debe proporcionar al clon un nuevo identificador del sistema de Oracle (SID). No se pueden ejecutar dos bases de datos con el mismo SID simultáneamente en el mismo host. Puede tener un clon en otro host que utiliza el mismo SID. Para designar un nombre único para el clon, utilice -label. Si no utiliza esta opción, SnapManager crea un nombre único para el clon que incluye el SID, fecha y hora.

Después de clonar una base de datos, es posible que desee actualizar los archivos tnsnames.ora en los equipos cliente con la nueva información de conexión de base de datos clonada. Los archivos tnsnames.ora se utilizan para conectarse a una instancia de Oracle sin tener que especificar la información completa de la base de datos. SnapManager no actualiza los archivos tnsnames.ora.

SnapManager siempre crea un backup, incluidos los archivos de registro de archivos, si se utiliza el perfil creado con backups -include-con-en-línea. SnapManager permite clonar únicamente los backups completos de la base de datos.

SnapManager (3.2 o posterior) permite clonar los backups que contienen los archivos de datos y los archivos de registro de archivos.

Si el registro de archivos está disponible desde una ubicación externa, puede especificar la ubicación externa durante la clonado para recuperar la base de datos clonada en un estado coherente. Debe asegurarse de que Oracle pueda acceder a la ubicación externa. No se admite la clonado de backups de solo registro de archivos.

Aunque se crea el backup de registros de archivos junto con el backup parcial en línea, no se puede crear un clon de la base de datos con este backup.

Es posible clonar el backup de base de datos desde la ubicación de archivo de registro de archivos externo solo para una base de datos independiente.

Se produce un error en la clonado del backup de la base de datos en línea de la base de datos de Real Application Clusters (RAC) mediante la ubicación del archivo de registro de archivos externo debido a un fallo en la recuperación. Esto se debe a que la base de datos de Oracle no puede encontrar y aplicar los archivos de registro de archivos para la recuperación desde la ubicación del registro de archivos externo al clonar el backup de la base de datos.

Puede especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de creación de clones con errores o correctamente.

Clonación de copia de seguridad de archivo de datos sin copia de seguridad de archivo de registro

Cuando el backup de archivos de datos no incluye el backup de registros de archivo, SnapManager para Oracle clona la base de datos según el número de cambio del sistema (SCN) registrado durante el backup. Si no se puede recuperar la base de datos clonada, se muestra el mensaje de error archivo de registro archivado de <number> de subproceso y <SCN> de cambio necesario para completar la recuperación, a pesar de que SnapManager para Oracle sigue clonando la base de datos y, finalmente, se realiza correctamente la creación del clon.

Al clonar con el backup de archivos de datos sin incluir el backup de registros de archivos, SnapManager recupera la base de datos clonada hasta el último SCN de registro de archivos, que se registra durante el backup.

1. Cree un archivo de especificación del clon.
2. Para crear un clon, introduzca el siguiente comando: smo clone create -backup-labelbackup_name -newsidnew_sid-labelclone_label-profileprofile_name-clonespecpath_to_clonespecfile [-taskspectaskspec] [-recover-from-location] path1 [,<path2>…][-dump]]

Información relacionada

Clonado de bases de datos en estado actual

Consideraciones para clonar una base de datos en un host alternativo

Creando especificaciones de clon

El comando smo clone create

Crear scripts de tareas previas, tareas posteriores y directivas

Variables disponibles en los scripts de tareas para la operación de clonado

Creación de scripts de tareas

Almacenamiento de los scripts de tareas

Clonado de bases de datos en estado actual

Puede crear un backup y un clon de la base de datos desde el estado actual de la base de datos mediante un solo comando.

Cuando especifica el perfil con la opción -current, SnapManager crea primero un backup y, a continuación, un clon del estado actual de la base de datos.

En la configuración de perfil, si habilitó el backup de archivos de datos y registros de archivos juntos para la clonado, siempre que se realice un backup de los archivos de datos en línea, también se realizará un backup de los registros de archivos. Al clonar la base de datos, SnapManager crea el backup de archivos de datos junto con el backup del registro de archivos y crea el clon de la base de datos. Si no se incluye el backup de registros de archivos, SnapManager no crea el backup de registros de archivos y, por lo tanto, no puede crear el clon de la base de datos.

1. Para clonar la base de datos en su estado actual, introduzca el siguiente comando: smo clone create -profileprofile_name-current -labelclone_name-clononpec./clonespec_filename.xml

   Este comando realiza un backup completo automático (generando la etiqueta de backup) e inmediatamente crea un clon a partir de ese backup mediante una especificación de clon existente que

desea utilizar.

> Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de las operaciones realizadas correctamente o con errores. El volcado se recoge tanto para las operaciones de backup como de clonado.

Clonado de backups de bases de datos sin necesidad de restablecer registros

SnapManager le permite realizar clonados flexibles, de modo que puede recuperar la base de datos clonada manualmente en un momento determinado sin necesidad de abrir la base de datos mediante reaslogs. También puede configurar manualmente la base de datos clonada como una base de datos en espera de Data Guard.

Cuando se puede seleccionar la opción -no-resetlogs mientras se crea el clon, SnapManager realiza las siguientes actividades para crear la base de datos clonada:

1. Ejecuta la actividad de tarea de preprocesamiento, si se especifica, antes de iniciar la operación de clonado
2. Crea la base de datos clonada con el SID especificado por el usuario
3. Ejecuta las sentencias SQL emitidas con la base de datos clonada.

   Sólo se ejecutan correctamente las sentencias SQL que se pueden ejecutar en estado de montaje.

4. Ejecuta la actividad de la tarea de posprocesamiento, si se especifica.

Qué tareas debe realizar para recuperar la base de datos clonada manualmente

1. Monte los backups de registros de archivos y recupere la base de datos clonada manualmente mediante los archivos de registro de archivos desde la ruta montada.
2. Después de realizar la recuperación manual, abra la opción recovery cloned database with -reaslogs.
3. Cree espacios de tablas temporales, si es necesario.
4. Ejecute la utilidad DBNEWID.
5. Conceda un privilegio sysdba a las credenciales de la base de datos clonada.

Mientras se clonan los backups de la base de datos mediante la opción -no-resetlogs, SnapManager deja la base de datos clonada en el estado montado para poder realizar una recuperación manual.

> La base de datos clonada creada con la opción -no-resetlogs no es una base de datos completa. Por lo tanto, no debe ejecutar ninguna operación de SnapManager en esta base de datos, si bien SnapManager no le restringe la posibilidad de realizar ninguna operación.

Si no se especifica la opción -no-resetlogs, SnapManager aplica los archivos de registro de archivos y abre la base de datos con resetlogs.

1. Introduzca el siguiente comando: smo clone create -profileprofile_name [-backup-labelbackup_name | -backup-idbackup_id | current] -newsidnew_sid-clonespecfull_path_to_clonespecfile-no-resetlogs

   Si intenta especificar las opciones -no-resetlogs y Recover-from-location, SnapManager no le permite especificar ambas opciones juntas y muestra el mensaje de error: SMO-04084: Debe especificar una de las opciones: -No-resetlogs o -recover-from-location.

Ejemplo

```
smo clone create -profile product -backup-label full_offline -newsid
PROD_CLONE -clonespec prod_clonespec.xml -label prod_clone-reserve -no
-reset-logs
```

Consideraciones para clonar una base de datos en un host alternativo

Para poder clonar en un host distinto al que reside la base de datos, deben cumplirse algunos requisitos.

En la siguiente tabla se muestran los requisitos de configuración del host de origen y de destino:

Requisitos previos de configuración	Requisito
Arquitectura	Debe ser igual en los hosts de origen y objetivo
Sistema operativo y versión	Debe ser igual en los hosts de origen y objetivo
SnapManager para Oracle	Se debe instalar y ejecutar en los hosts de origen y objetivo
Credenciales	Se debe configurar para que el usuario acceda al host de destino
Oracle	Se debe instalar la misma versión de software en los hosts de origen y destino. Oracle Listener debe ejecutarse en el host de destino.
Pila de almacenamiento compatible	Debe ser igual en los hosts de origen y objetivo
Protocolo utilizado para acceder a los archivos de datos	Debe ser igual en los hosts de origen y objetivo
Gestores de volúmenes	Debe configurarse en los hosts de origen y destino y debe tener versiones compatibles

También es posible clonar una base de datos de Automatic Storage Management (ASM) en un host remoto. Cuando lo haga, debe asegurarse de que la instancia de ASM esté en ejecución en el host remoto.

Clonar una base de datos en un host alternativo

Puede utilizar el comando clone create para clonar un backup de base de datos en un host alternativo.

- Cree un perfil o tenga un perfil existente.

- Crear una copia de seguridad completa o tener una copia de seguridad de la base de datos existente.
- Cree una especificación de clon o tenga una especificación de clon existente.
  a. Para clonar una base de datos en un host alternativo, introduzca el siguiente comando: smo clone create -backup-label backup_label_name-newsid new_sid-host target_host-label clone_label-commentcomment_text-profileprofile_name-clonefilespec full_path_to_clonesfile

     Oracle no permite ejecutar dos bases de datos con el mismo SID simultáneamente en el mismo host. Por este motivo, debe suministrar un SID nuevo para cada clon. Sin embargo, puede tener una base de datos en otro host con el mismo SID.

Información relacionada

Creación de perfiles

Clonar bases de datos a partir de backups

Creando especificaciones de clon

El comando smo clone create

Ver una lista de clones

Puede ver una lista de clones asociados con un perfil determinado.

La lista incluye la siguiente información sobre los clones de un perfil:

- El ID del clon
- Estado de la operación de clonado
- SID de Oracle para el clon
- Host donde reside el clon
- Etiqueta del clon

Si especifica la opción -verbose, la salida también muestra los comentarios introducidos para el clon.

1. Para mostrar una lista de todos los clones de un perfil, introduzca el siguiente comando smo clone list -profile_name [-quiet | -verbose]

Información relacionada

El comando smo clone list

Visualización de información detallada de los clones

Puede ver información detallada sobre un clon específico mediante el comando clone show.

El comando clone show muestra la siguiente información:

- Identificador del sistema del clon e ID del clon
- Estado de la operación de clonado

- Clonar crear fecha y hora de inicio y finalización
- Etiqueta del clon
- Clonar comentario
- Etiqueta e ID de copia de seguridad
- Base de datos de origen
- Hora de inicio y de finalización de la copia de seguridad
- Nombre de la base de datos, tablespaces y archivos de datos
- El nombre del host y los sistemas de archivos que contienen archivos de datos
- Los volúmenes del sistema de almacenamiento y las copias Snapshot respaldan el clon
- Si el clon se creó con el backup en el almacenamiento primario o secundario

  a. Introduzca el siguiente comando: `smo clone show -profile profile_name [-label label | -id guid]`

Información relacionada

El comando smo clone show

Eliminar clones

Puede eliminar los clones cuando el tamaño de la copia Snapshot alcance entre un 10% y un 20% del backup. Así también se garantiza que el clon tenga los datos más recientes.

La etiqueta es el identificador único de cada clon en un perfil. Puede usar la etiqueta o el ID del clon, pero no el identificador del sistema (SID) para eliminar el clon.

> El SID del clon y la etiqueta del clon no son iguales.

Cuando elimina un clon, la base de datos debe estar en ejecución. De lo contrario, no se eliminarán muchos ficheros y directorios del clon existente, lo que hará que se realice más trabajo antes de crear otro clon.

Los directorios especificados para ciertos parámetros de Oracle del clon se destruyen cuando se elimina el clon y solo deben contener datos para la base de datos clonada: Destinos de registro de archivo, destinos de fondo, núcleo y destinos de volcado de usuario. No se eliminan los archivos de auditoría.

> No es posible eliminar un clon cuando se utiliza en otras operaciones.

Opcionalmente, es posible recoger los archivos de volcado después de una operación de eliminación de clonado correcta o con errores.

1. Introduzca el siguiente comando: smo clone delete -profile profile_name [-label label label label | -id guid] [-sysspasswordsyspassword]| [login-usernamedb_username-password] dB_password-portdb_Port] [-asminstance-asmusernameTM_username-aspasswordasma_password][-verbose][-verbose][-verbose]]

Ejemplo

```
smo clone delete -profile targetdb1_prof1 -label sales0908_clone1
```

Información relacionada

El comando smo clone delete

Dividir un clon

SnapManager le permite dividir y gestionar un clon existente creado mediante la tecnología FlexClone. En la tecnología FlexClone, el clon y la base de datos original comparten los mismos bloques de datos físicos.

Antes de ejecutar la operación de división de clones, puede saber que el tamaño estimado del clon se dividirá y el espacio requerido disponible en el agregado.

SnapManager genera un nuevo perfil si la operación de división de clones se realiza correctamente. Si SnapManager no puede crear el nuevo perfil, puede crear manualmente un nuevo perfil. Puede utilizar el nuevo perfil para crear backups de bases de datos, restaurar datos y crear clones. Si la operación de división de clones se realiza correctamente, independientemente de si se crea el perfil nuevo o no, los metadatos relacionados con la clonado se eliminan de la base de datos del repositorio.

Puede realizar las siguientes tareas relacionadas con la división de clones:

- Ver la estimación de división de clones.
- Divida un clon en un almacenamiento primario.
- Divida un clon en un almacenamiento secundario.
- Ver el estado de la operación de división de clones.
- Detenga la operación de división de clones.
- Destruir el perfil junto con el almacenamiento subyacente.
- Elimine el perfil creado para un clon dividido.

Cuando divide un clon de su volumen principal, se eliminan las copias Snapshot asociadas con el volumen clonado. No se pueden utilizar los backups creados para la base de datos clonada antes del proceso de división de clones porque las copias de Snapshot de estos backups se eliminan y los backups permanecen como entradas obsoletas en el repositorio.

Ver una estimación de división de clones

La estimación de división de clones ayuda a conocer el espacio libre total disponible en el agregado, la cantidad de espacio compartido entre el clon y la base de datos original, y el espacio utilizado exclusivamente por el clon. Además, puede ver la fecha y la hora en que se creó el clon subyacente y la antigüedad del clon. Según esta estimación, usted decide si dividir un clon o no.

Para ver la estimación de división de clones, debe introducir el nombre del perfil del clon original y la etiqueta o GUID de la operación de clonado. Si el clon está en otro host, es posible especificar el nombre de host.

1. Para ver la estimación de división de clones, introduzca el siguiente comando: `smo clone split-`

```
estimate -profileprofile [-hosthostname] [-labelclone-label | -idclone-id][
-quiet | -verbose]
```

En el siguiente ejemplo, se muestra el comando para la estimación de almacenamiento de división de clones:

```
smo clone split-estimate

-profile p1 -label clone_test_label
```

Dividir un clon en el almacenamiento principal o secundario

Puede usar el comando clone split para dividir el clon. Una vez finalizada la división de clones, los metadatos del clon se eliminan de la base de datos del repositorio y es posible eliminar o liberar el backup asociado con el clon.

El nuevo perfil creado después de la operación de división correcta se utiliza para gestionar el clon de división. El nuevo perfil será como cualquier otro perfil existente en SnapManager. Este perfil se puede usar para llevar a cabo operaciones de backup, restauración y clonado.

Además, también es posible configurar las notificaciones por correo electrónico para el nuevo perfil. Esto permite al administrador de la base de datos recibir notificaciones sobre el estado de la operación de la base de datos realizada mediante el perfil.

SnapManager admite la operación de separación cuando se realiza únicamente en FlexClone.

Si la operación de división falla, se muestra un mensaje de error adecuado con el motivo del fallo. El estado de varias operaciones también se muestra en el registro de operaciones. Por ejemplo:

```
--[ INFO] The following operations were completed:
Clone Split : Success
Profile Create : Failed
Clone Detach : Success
```

Opcionalmente, es posible recoger los archivos de volcado después de una operación de división de clones realizada correctamente o con errores.

Después de introducir el comando de división de clones, no debe detener el servidor SnapManager hasta que se haya iniciado la operación de división de clones.

SnapManager genera el perfil aunque no proporcione ningún valor para la cuenta de Oracle (osaccount y osgroup).

1. Escriba el siguiente comando: smo clone split -recprofilone-profile-hotthostname [-labelclone-label | -idclone-id]-split-labelsplit-operation-label-commentnew-profilenew-profile-name [-profile-profile-profile-dbnepo_nombre_nombre_host] [-nombre_nombre_nombre_nombre_host]-nombre_nombre_nombre_nombre_usuariob]-nombre_nombre_nombre_nombre_nombre_nombre_archivo]-nombre_nombre_nombre_usuario_nombre_nombre_nombre_archivo]-nombre_archivo-

nombre_nombre_nombre_archivo_archivo] [-nombre_usuario_archivo_archivo_archivo_archivo_nombre_nombre_nombre_nombre_archivo]-nombre_usuario_usuario_nombre_nombre_archivo]-nombre_nombre_nombre_archivo]-nombre_usuario_archivo_nombre_nombre_nombre_archivo_archivo_archivo] [-nombre_usuario_archivo_archivo_archivo_archivo_archivo_archivo_archivo_archivo_archivo_archivo_nombre_nombre_nombre_archivo]-nombre_

Ver el estado del proceso de división de clones

Puede ver el progreso del proceso de división iniciado.

1. Para ver el progreso del proceso de división de clones, introduzca el siguiente comando: `smo clone split-status -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-status -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Ver el resultado del proceso de división de clones

Es posible ver el resultado del proceso de división de clones iniciado.

1. Para ver el resultado del proceso de división de clones, introduzca el siguiente comando: `smo clone split-result -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-result -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Detener el proceso de división de clones

Es posible detener el proceso de división de clones en ejecución.

Después de detener el proceso de división, no podrá reanudarlo.

1. Para detener la operación de división de clones, introduzca el siguiente comando: `smo clone split-stop -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-stop -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Eliminación de un perfil

Es posible eliminar un perfil siempre que no contenga backups correctos que se estén utilizando actualmente en otras operaciones. Es posible eliminar perfiles que contengan copias de seguridad liberadas o eliminadas.

1. Introduzca el siguiente comando: `smo profile delete -profileprofile [-quiet | -verbose]`

Es posible eliminar un nuevo perfil creado para la división de clones. Mientras se elimina, Si elimina el perfil, no puede destruir el perfil más tarde se muestra el mensaje de advertencia en la interfaz de línea de comandos de SnapManager.

```
smo profile delete -profile AUTO-REVEN
```

Destruir un perfil

SnapManager permite destruir el perfil asociado con el clon dividido (base de datos) junto con el almacenamiento subyacente. Antes de destruir el perfil, asegúrese de eliminar los backups y clones asociados.

1. Para destruir un perfil creado con la operación de división de clones y la base de datos de división de clones, introduzca el siguiente comando: `smo profile destroy -profileprofile [-hosthostname] [-quiet | -verbose]`

```
smo profile destroy -profile AUTO-REVEN
```

Eliminar un ciclo de operaciones de división de clones de una base de datos de repositorio

Puede eliminar una entrada de ciclo de operaciones de división de clones desde una base de datos de repositorio.

1. Para eliminar una entrada del ciclo de operaciones de división de clones de una base de datos de repositorio, introduzca el siguiente comando:smo clone split-delete -profileprofile [-hoshostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]

```
smo clone split-delete -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Introducción a la protección de datos en SnapManager

SnapManager admite protección de datos para proteger los backups en sistemas de almacenamiento secundarios o terciarios. Debe configurar las relaciones de SnapMirror y SnapVault entre los volúmenes de origen y de destino.

Si se utiliza Data ONTAP en 7-Mode, SnapManager ofrece protección de datos condicionada por políticas al integrarse con Protection Manager (OnCommand Unified Manager). De este modo se automatiza la replicación de backups de SnapManager en un sistema de almacenamiento principal a un sistema de almacenamiento secundario o incluso a un sistema de almacenamiento terciario gracias a las políticas de SnapVault o SnapMirror creadas por el administrador de almacenamiento o backup en Protection Manager. La retención en el almacenamiento principal es controlada por SnapManager según la retención definida durante la creación de perfiles y la clase de retención etiquetada durante la creación de backups. La retención de los backups de almacenamiento secundario es controlada por la política definida en Protection Manager.

Si utiliza Clustered Data ONTAP, SnapManager 3.4 proporciona políticas de *SnapManager_CDOT_Mirror* y *SnapManager_CDOT_Vault* para la protección de datos. Al crear un perfil, puede seleccionar estas políticas

en función de la relación de SnapMirror o SnapVault que se haya establecido mediante la CLI de Clustered Data ONTAP o System Manager. Cuando se crea un backup, en el que se selecciona el perfil para el cual se habilita la protección, los backups se protegen en un sistema de almacenamiento secundario.

Si utilizaba SnapManager 3.3.1 con Clustered Data ONTAP, los backups estaban protegidos usando secuencias de comandos posteriores que se seleccionaron al crear perfiles. Si desea utilizar esos perfiles, después de actualizar a SnapManager 3.4, debe realizar las siguientes operaciones.

- Debe actualizar los perfiles para seleccionar la política *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault* y eliminar el script posterior que se utilizó para la protección de datos.
- Después de actualizar el perfil para utilizar la política *SnapManager_CDOT_Vault*, debe eliminar las programaciones de backup existentes y crear nuevas programaciones para especificar la etiqueta de SnapVault para los backups.
- Si los perfiles se crearon en SnapManager 3.3.1 sin seleccionar los scripts posteriores, debe actualizar los perfiles para seleccionar la política *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault* para habilitar la protección de datos.

> Si tiene backups en el sistema de almacenamiento secundario que fueron reflejados o en almacén con scripts posteriores de SnapManager 3.3.1, no podrá utilizar dichos backups para restaurar o clonar con SnapManager 3.4.

Si utiliza Clustered Data ONTAP, SnapManager 3.4.2 admite varias relaciones de protección (SnapMirror y SnapVault) en los volúmenes de origen. Solo se admiten una relación de SnapMirror y una relación de SnapVault por volumen. Debe crear perfiles independientes, cada uno con el SnapManager_CDOT_Mirror y la política de SnapManager_CDOT_Vault seleccionada.

> SnapDrive para Unix 5.3.2 y posterior es necesario para usar múltiples políticas de protección.

¿Qué son las políticas de protección

Las políticas de protección son reglas que rigen el modo en que se protegen los backups de la base de datos. Puede seleccionar las políticas de protección mientras crea el perfil.

Una política de protección define los siguientes parámetros:

- El momento de transferir copias a un almacenamiento secundario
- La cantidad máxima de datos que se deben transferir a las horas programadas
- El tiempo de retención de las copias de cada ubicación de respaldo
- Umbrales de advertencia y error para tiempos de retraso

Cuando la protección está habilitada, SnapManager crea un conjunto de datos para la base de datos. Un conjunto de datos consta de una colección de conjuntos de almacenamiento junto con la información de configuración asociada con sus datos. Los conjuntos de almacenamiento asociados a un conjunto de datos incluyen un conjunto de almacenamiento principal utilizado para exportar datos a clientes y el conjunto de réplicas y archivos que existen en otros conjuntos de almacenamiento. Los conjuntos de datos representan datos de usuario exportables. Si el administrador deshabilita la protección de una base de datos, SnapManager elimina el conjunto de datos.

Qué estados de protección son

SnapManager muestra el estado de cada backup. Los administradores deben conocer los distintos estados y supervisar el estado de sus backups.

Un backup de la base de datos puede tener los siguientes estados de protección:

Estado	Definición	Explicación
Protegido	Se solicitó protección y se ha activado.	La protección está habilitada para el backup en SnapManager y Protection Manager copió correctamente el backup en otro conjunto de discos físicos (también denominado almacenamiento secundario). Si Protection Manager quita un backup del almacenamiento secundario debido a una política de retención, puede que el backup regrese a un estado no protegido.
Sin proteger	Se solicitó protección, pero no se completó.	La protección se habilita para el backup, pero el backup no se copia en otro conjunto de discos físicos. El backup aún no está protegido o falló la protección, o estaba protegido antes, pero ya no está protegido. Cuando se crea un backup, el estado de protección inicial del backup no se solicita o no está protegido. Si el backup no está protegido, se protege al transferirse a un almacenamiento secundario.
No solicitado	No se solicitó protección.	La protección no está habilitada para el backup. Existe una copia lógica de los datos en los mismos discos físicos (también conocidos como backup local). Si el backup no se solicita con la protección, la protección del backup siempre se muestra como no solicitada.

Qué pools de recursos son

Un pool de recursos es una colección de almacenamiento físico sin usar (como sistemas de almacenamiento o agregados) del cual se pueden aprovisionar volúmenes o LUN nuevos para contener datos. Si asigna un sistema de almacenamiento a un pool de recursos, todos los agregados de ese sistema de almacenamiento se mostrarán

disponibles para el aprovisionamiento.

Los administradores de almacenamiento usan la consola de Protection Manager para asignar un conjunto de recursos a las copias de respaldo y de duplicación. La aplicación de aprovisionamiento puede entonces aprovisionar automáticamente volúmenes fuera de los recursos físicos del conjunto de recursos para contener backups y copias de mirroring.

Para perfiles protegidos, SnapManager muestra información sobre un perfil e indica si se ha asignado un conjunto de recursos de almacenamiento a ese perfil. Si no es así, el perfil se considera "no conforme". Tras asignar un pool de recursos de almacenamiento al conjunto de datos del perfil correspondiente, el perfil se considera "conforme".

Acerca de diferentes políticas de protección

Puede seleccionar diferentes políticas para proteger los backups en los sistemas de almacenamiento secundario o terciario.

Si utiliza Data ONTAP en 7-Mode y SnapManager se integra con Protection Manager, debe seleccionar una de las siguientes políticas de protección al crear el perfil. La consola de gestión de Protection Manager proporciona plantillas para configurar políticas de protección de los conjuntos de datos. Aunque las políticas de protección de recuperación tras desastres se enumeran en la interfaz de usuario de SnapManager, estas políticas no son compatibles.

Política	Descripción
Realice un backup	Mediante SnapVault o SnapMirror, se realiza un backup de un conjunto de datos de forma local y también del almacenamiento principal al secundario.
Realice copias de seguridad y, a continuación, haga mirroring	Se realiza un backup de un conjunto de datos del almacenamiento primario al secundario mediante SnapVault o SnapMirror, y luego se crea mirroring en un partner de SnapMirror.
Únicamente copias Snapshot locales	Un conjunto de datos solo utiliza copias Snapshot locales en el almacenamiento principal.
Replicación	Un conjunto de datos se refleja del almacenamiento primario al secundario mediante SnapMirror.
Mirroring y backup	Mediante SnapMirror, un conjunto de datos se refleja del almacenamiento primario al secundario y, a continuación, se realiza un backup en el almacenamiento secundario mediante SnapVault o SnapMirror.
Espejo y espejo	Un conjunto de datos se refleja del almacenamiento principal al secundario en dos partners de SnapMirror distintos.

Política	Descripción
Mirror, y, a continuación, backup	Mediante SnapMirror, un conjunto de datos se refleja del almacenamiento principal al secundario y, posteriormente, se realiza un backup del mismo a un almacenamiento terciario mediante SnapVault o SnapMirror.
Haga simetría y, a continuación, haga simetría	Un conjunto de datos se refleja del almacenamiento primario al secundario mediante SnapMirror y, a continuación, se refleja en un partner de SnapMirror adicional.
Sin protección	Un conjunto de datos no tiene copias Snapshot, backups ni protección contra copias reflejadas de ningún tipo.
Solo backup remoto	Mediante SnapVault o SnapMirror, se realiza un backup de los datos en un sistema de almacenamiento de forma remota a un almacenamiento secundario. La aplicación con licencia no realiza backups locales en el almacenamiento primario. Esta política de protección se puede aplicar a sistemas de terceros con Open Systems SnapVault instalado.

Si utiliza Clustered Data ONTAP, debe seleccionar una de las siguientes políticas de protección mientras crea el perfil.

Política	Descripción
SnapManager_CDOT_Mirror	Duplica el backup.
SnapManager_CDOT_Vault	Almacena la copia de seguridad.

Configuración y habilitación de la protección de datos condicionada por políticas

Debe configurar SnapDrive y DataFabric Manager Server para permitir la protección de datos en el perfil a fin de proteger backups en sistemas de almacenamiento secundario. Puede seleccionar las políticas de protección en la consola de Protection Manager para especificar cómo se protegerán los backups de la base de datos.

> Debe asegurarse de que Unified Manager de OnCommand se encuentre instalado en un servidor aparte para habilitar la protección de datos.

Configuración de DataFabric Manager Server y SnapDrive cuando el control de acceso basado en roles está habilitado

Cuando se habilita el control de acceso basado en roles (RBAC), debe configurar

DataFabric Manager Server para que incluya las funcionalidades de RBAC. También debe registrar al usuario de SnapDrive creado en DataFabric Manager Server y al usuario raíz del sistema de almacenamiento en SnapDrive.

1. Configure DataFabric Manager Server.
   a. Para actualizar DataFabric Manager Server para actualizar los cambios realizados directamente en el sistema de almacenamiento por la base de datos de destino, introduzca el siguiente comando:dfm host Discover Storage_System
   b. Cree un usuario nuevo en DataFabric Manager Server y defina la contraseña.
   c. Para añadir el usuario del sistema operativo a la lista de administración del servidor DataFabric Manager, introduzca el siguiente comando: dfm user add sd-admin
   d. Para crear una nueva función en DataFabric Manager Server, introduzca el siguiente comando:dfm role create sd-admin-role
   e. Para agregar la funcionalidad DFM.Core.AccessCheck Global a la función, introduzca el siguiente comando:rol dfm add sd-admin-role DFM.Core.AccessCheck Global
   f. Para agregar sd-admin-role al usuario del sistema operativo, introduzca el siguiente comando:dfm user role set sd-adminsd-admin-role
   g. Para crear otra función en DataFabric Manager Server para el usuario raíz de SnapDrive, introduzca el siguiente comando:dfm role create sd-Protect
   h. Para agregar funciones de RBAC a la función creada para el usuario raíz de SnapDrive o el administrador, escriba los siguientes comandos:rol dfm add sd-Protect SD.Config.Read Globaldfm role add sd-Protect SD.Config.Write Globaldfm role add sd-Protect SD.Config.GlobalDelete dfm rol add sd-Protect SD.Storage.Read Globaldfm función add.sd-Protect
   i. Para añadir el usuario de oracle de la base de datos de destino a la lista de administradores del servidor DataFabric Manager y asignar la función sd-Protect, escriba el siguiente comando:dfm user add -r sd-protecttardb_host1\oracle
   j. Para añadir el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, introduzca el siguiente comando:dfm host set Storage_System hostLogin=oracle hostPassword=password
   k. Para crear una nueva función en el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, introduzca el siguiente comando:dfm host role create -h Storage_System-c "api-**, login-**" Storage-rbac
   l. Para crear un nuevo grupo en el sistema de almacenamiento y asignar el nuevo rol creado en DataFabric Manager Server, introduzca el siguiente comando:dfm host usergroup create -h Storage_System-r Storage-rbac-roleStorage-rbac-group
   m. Para crear un nuevo usuario en el sistema de almacenamiento y asignar la nueva función y el grupo creado en DataFabric Manager Server, introduzca el siguiente comando:dfm host user create -h Storage_system-r Storage-rbac-role -p password -g Storage-rbac-groupptardb_host1
2. Configure SnapDrive.
   a. Para registrar las credenciales del usuario sd-admin en SnapDrive, introduzca el siguiente comando:snapdrive config set -dfm sd-admindfm_host
   b. Para registrar el usuario raíz o el administrador del sistema de almacenamiento con SnapDrive, introduzca el siguiente comando:snapdrive config set tardb_host 11erorage_system

La configuración de SnapDrive cuando RBAC no está habilitado

Para habilitar la protección de datos, debe registrar en SnapDrive al usuario raíz o al administrador de DataFabric Manager Server y al usuario raíz del sistema de almacenamiento.

1. Para actualizar DataFabric Manager Server para actualizar los cambios realizados directamente en el sistema de almacenamiento mediante la base de datos de destino, introduzca el siguiente comando:

   host dfm detecte storage_system

2. Para registrar el usuario raíz o el administrador de DataFabric Manager Server en SnapDrive, introduzca el siguiente comando:

   SnapDrive config set -dfm Administratordfm_host

3. Para registrar el usuario raíz o el administrador del sistema de almacenamiento con SnapDrive, escriba el siguiente comando:

   configuración de SnapDrive establezca root storage_system

Comprender la habilitación o deshabilitación de la protección de datos en el perfil

Puede habilitar o deshabilitar la protección de datos al crear o actualizar un perfil de base de datos.

Para crear un backup protegido de una base de datos en los recursos de almacenamiento secundario, los administradores de bases de datos y los administradores de almacenamiento realizan las siguientes acciones.

Si desea…	Realice lo siguiente…
Cree o edite un perfil	Para crear o editar un perfil, realice lo siguiente: • Habilite la protección de backup en el almacenamiento secundario. • Si utiliza Data ONTAP en 7-Mode y tiene instalado Protection Manager, puede seleccionar las políticas creadas por el administrador de almacenamiento o backup en Protection Manager. Si utiliza Data ONTAP en 7-Mode y la protección está habilitada, SnapManager crea un conjunto de datos para la base de datos. Un conjunto de datos consta de una colección de conjuntos de almacenamiento junto con la información de configuración asociada con sus datos. Los conjuntos de almacenamiento asociados a un conjunto de datos incluyen un conjunto de almacenamiento principal utilizado para exportar datos a clientes y el conjunto de réplicas y archivos que existen en otros conjuntos de almacenamiento. Los conjuntos de datos representan datos de usuario exportables. Si el administrador deshabilita la protección de una base de datos, SnapManager elimina el conjunto de datos. • Si utiliza ONTAP, debe seleccionar la política *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault_* en función de la relación de SnapMirror o SnapVault creada. Al deshabilitar la protección de copia de seguridad, se muestra un mensaje de advertencia que indica que el conjunto de datos se eliminará y no será posible restaurar o clonar copias de seguridad para este perfil.
Ver el perfil	Dado que el administrador de almacenamiento aún no ha asignado recursos de almacenamiento para implementar la normativa de protección, el perfil se muestra como no conforme tanto en la interfaz gráfica de usuario de SnapManager como en el resultado del comando profile show.

Si desea…	Realice lo siguiente…
Asigne recursos de almacenamiento en la consola de gestión de Protection Manager	En Protection Manager Management Console, el administrador de almacenamiento ve el conjunto de datos no protegido y asigna un pool de recursos a cada nodo del conjunto de datos que está asociado con el perfil. A continuación, el administrador de almacenamiento garantiza que los volúmenes secundarios estén aprovisionados y que se inicialicen las relaciones de protección.
Ver el perfil conforme en SnapManager	En SnapManager, el administrador de la base de datos ve que el perfil ha cambiado al estado conforme tanto en la interfaz gráfica de usuario como en la salida del comando profile show, lo que indica que se han asignado recursos.
Cree el backup	• Seleccione Full backup. • Además, seleccione si el backup debe estar protegido y seleccione la clase de retención primaria (por ejemplo, por hora o por día). • Si utiliza Data ONTAP operando en 7-Mode y desea proteger el backup inmediatamente en un almacenamiento secundario, lo que anula la programación de protección de Protection Manager, especifique la opción -protectnow. • Si utiliza ONTAP y desea proteger el backup inmediatamente en el almacenamiento secundario, especifique la opción Protect. La opción protectnow no se puede aplicar en Clustered Data ONTAP.
Vea el backup	El nuevo backup se muestra como programado para la protección, pero no está protegido (en la interfaz SnapManager y en el resultado del comando backup show). El estado de protección se muestra como «"no protegido"».
Consulte la lista de copias de seguridad	Una vez que el administrador de almacenamiento haya verificado que el backup se ha copiado a un sistema de almacenamiento secundario, SnapManager cambia el estado «sin protección» a «protegido».

Cómo SnapManager retiene los backups en el almacenamiento local

SnapManager permite crear backups que cumplen las políticas de retención, lo cual especifica cuántos backups se deben conservar correctamente en el almacenamiento

local. Puede especificar la cantidad de backups correctos que debe conservarse en el perfil de una determinada base de datos.

Es posible crear backups para lo siguiente:

- 10 días de backup diarios en almacenamiento primario
- 2 meses de backups mensuales en almacenamiento primario
- 7 días de backup diarios en almacenamiento secundario
- 4 semanas de backups semanales en el almacenamiento secundario
- 6 meses de backups mensuales en almacenamiento secundario

Para cada perfil de SnapManager, puede cambiar los valores de las siguientes clases de retención no limitadas:

- Cada hora
- Todos los días
- Semanal
- Mensual

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Un backup caduca cuando su antigüedad supera el período de retención establecido para su clase de retención o la cantidad de backups supera el número de retenciones. Por ejemplo, si el número de backup es 15 (SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups elegibles más antiguos caducan.

Cuando se caduca un backup, SnapManager libera o elimina el backup caducado. SnapManager siempre conserva el último backup realizado.

SnapManager solo cuenta la cantidad de backups realizados correctamente para el número de retención y no considera lo siguiente:

Backups no incluidos en el número de retención	Detalles adicionales
Backups con errores	SnapManager conserva la información sobre backups realizados correctamente y sin errores. Aunque los backups sin éxito requieren solo un espacio mínimo en el repositorio, es posible que desee eliminarlos. Los backups sin éxito permanecen en el repositorio hasta que se eliminan.
Backups designados para retenerse en cuenta de forma ilimitada o con backups para otra clase de retención	SnapManager no elimina los backups designados para que se conserven de forma ilimitada. Además, SnapManager solo considera los backups en la misma clase de retención (por ejemplo, SnapManager sólo considera los backups por horas para el número de retención por horas).

Backups no incluidos en el número de retención	Detalles adicionales
Backups montados desde el almacenamiento local	Cuando se montan las copias Snapshot, también se clonan y por lo que no se consideran aptos para la retención. SnapManager no puede eliminar las copias Snapshot si están clonadas.
Backups que se utilizan para crear un clon en el almacenamiento local	SnapManager conserva todos los backups que se usan para crear clones, pero no los considera para el número de retención de backups.
Backups que se clonan o se montan en un almacenamiento secundario y que utilizan la política de protección de reflejos	Si SnapManager elimina las copias Snapshot para el backup en el recurso de almacenamiento primario y se duplican las copias Snapshot, producirá un error en el próximo backup en el almacenamiento secundario.

Cuando se libera un backup de sus recursos de almacenamiento primario, se destruyen los recursos primarios (copias Snapshot) utilizados por el backup, pero los metadatos de backup siguen estando disponibles. SnapManager no considera los backups liberados en el número de retención de backups.

SnapManager proporciona un recuento de retención y una duración predeterminados para cada clase de retención. Por ejemplo, para el recuento de clases de retención cada hora, SnapManager, de forma predeterminada, retiene cuatro backups por hora. Puede anular estos valores predeterminados y establecer los valores al crear o actualizar el perfil, o cambiar los valores predeterminados para el recuento de retenciones y la duración en el archivo smo.config.

Los backups en el almacenamiento primario se pueden proteger mediante la realización de backups en el almacenamiento secundario. Mientras SnapManager gestiona la retención y la programación de backups en el almacenamiento principal, Protection Manager gestiona la retención y la programación de los backups en el almacenamiento secundario.

Cuando los backups locales caducan en función de su política de retención, se eliminan o se liberan, en función de si están protegidos.

- Si están protegidos, se liberan los backups locales. Sus recursos de almacenamiento o las copias Snapshot se eliminan, pero los backups permanecen en el repositorio de SnapManager y están disponibles para su restauración desde el almacenamiento secundario. No es necesario liberar backups (por ejemplo, con el comando backup libre). Los backups se liberan hasta que el backup ya no exista en el almacenamiento secundario y, en ese momento, se elimina el backup.
- Si no están protegidos, los backups locales se eliminan.

En una operación de backup solo de archivado, SnapManager no archiva los archivos de registro de recuperación, a diferencia del proceso de backup de base de datos en línea. Debe agregar una secuencia de comandos de pretarea para archivar los archivos redo log antes de realizar la operación de copia de seguridad de archivvelog-only. La secuencia de comandos de pretarea debe ejecutar el comando ALTER System switch logfile.

El siguiente ejemplo muestra las acciones que SnapManager realiza en diversos tipos de backups, según una política de retención de backups de tres días (con el número establecido en retener 3):

Fecha de la copia de seguridad	Estado	Se han adoptado medidas para la política de retención	Explicación
5/10	Exitoso	Mantenga	Este es el backup exitoso más reciente, por lo que se mantendrá.
5/9	Clonado correcto	Omitir	SnapManager no considera los backups utilizados para la clonado en el número de políticas de retención. Este backup se omite del número de backups realizados correctamente.
5/8	Correcto, montado	Omitir	SnapManager no considera los backups montados en el número de políticas de retención. Este backup se omite del número de backups realizados correctamente.
5/7	Error	Omitir	Los backups con errores no se cuentan.
5/5	Exitoso	Mantenga	SnapManager mantiene este segundo backup diario de éxito.
5/3	Exitoso	Mantenga	SnapManager mantiene este tercer backup diario de éxito.
5/2	Exitoso	Eliminar	SnapManager cuenta este backup correctamente, pero después de que SnapManager alcanza tres backups diarios correctos, este backup se elimina.

Información relacionada

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Aspectos que se deben tener en cuenta al realizar la protección de datos

Debe tener en cuenta ciertas consideraciones para realizar la protección de datos.

- Para realizar operaciones de clonado o restauración desde sistemas secundarios, se debe montar el volumen de destino en el espacio de nombres y exportarlo correctamente.
- Para deshabilitar el parámetro SnapDrive Configuration, compruebe-export-permision-nfs-clone, debe establecer el valor como off.

  La documentación de SnapDrive para UNIX en el sitio de soporte de NetApp contiene información adicional sobre el parámetro check-export-permision-nfs-clone.

- Debe configurar la relación de SnapMirror para los volúmenes de almacenamiento secundario solicitados en el sistema de almacenamiento secundario.
- Debe configurar la relación de SnapVault para los qtrees de almacenamiento secundario solicitados en el sistema de almacenamiento secundario para Data ONTAP que funciona en 7-Mode.
- Debe definir una política y reglas para la etiqueta de SnapMirror definida por el usuario si utiliza SnapVault post-script para Clustered Data ONTAP.

  La copia posterior de SnapVault es compatible con los volúmenes de Clustered Data ONTAP y los tipos de relación de SnapMirror DP y XDP. La documentación de ONTAP en el sitio de soporte de NetApp contiene información sobre la configuración de SnapMirror y SnapVault.

- En entornos NAS, debe configurar la ruta de datos NAS primaria y secundaria mediante el comando SnapDrive config set-mgmtpathManagement_pathManagement_pathManagement_pathdata_PATH.

  Por ejemplo, SnapDrive config set -mgmtpath f3050-197-91 f3050-197-91 f3050-197-91 f3050-220-91, donde `f3050-197-91` es la ruta de gestión y. `f3050-220-91` es la ruta de datos.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Licencias necesarias para la protección de datos en SnapManager

Debe asegurarse de que las licencias requeridas para la protección de datos estén instaladas y habilitadas en los sistemas de almacenamiento primario y secundario.

Los sistemas de almacenamiento primario reciben las últimas actualizaciones de transacciones para la base de datos Oracle, almacenan los datos y proporcionan protección de copia de seguridad local de la base de datos. El sistema de almacenamiento principal también conserva los archivos de datos de la base de datos, los archivos de registro y los archivos de control. Los sistemas de almacenamiento secundario actúan como almacenamiento remoto para los backups protegidos.

Para la protección de datos, deben instalarse y activarse las siguientes licencias en los sistemas de almacenamiento primario:

> Si desea habilitar la protección de datos en los sistemas de almacenamiento secundario, también debe instalar y habilitar estas licencias en los sistemas de almacenamiento secundario.

- Data ONTAP funcionando en 7-Mode (7.3.1 o posterior) o en Clustered Data ONTAP (8.2 o posterior)
- SnapVault (en función de la política de protección)
- SnapRestore

- SnapMirror (en función de la política de protección)
- Se requiere FlexClone para el sistema de archivos de red (NFS) yla clonación.

  Además, FlexClone es necesario para la red de área de almacenamiento (SAN) solo si SnapDrive está configurado para utilizar FlexClone en entornos SAN.

- El protocolo adecuado, por ejemplo, NFS, Internet Small Computer System Interface (iSCSI) o Fibre Channel (FC).

SnapVault o SnapMirror deben estar en los sistemas de almacenamiento primario y secundario en función de las políticas de protección utilizadas. Las políticas de protección de backup básicas requieren únicamente SnapVault instalado en los sistemas de soporte. Las políticas que incluyen protección con mirroring requieren la instalación de SnapMirror en los sistemas de soporte. Las políticas de recuperación ante desastres de backup y mirroring requieren la instalación de SnapMirror en los sistemas de soporte.

Protección de backups de bases de datos en almacenamiento secundario o terciario

Puede usar SnapManager para proteger las copias de backup en sistemas de almacenamiento secundarios o terciarios.

1. Introduzca el siguiente comando: `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]`

Si desea…	Realice lo siguiente…
Cree una copia de seguridad de una base de datos en línea o sin conexión, en lugar de permitir que SnapManager administre si está en línea o sin conexión	Especifique la opción -offline o -online para crear un backup de la base de datos sin conexión o la base de datos en línea. Si utiliza la opción -offline o -online, no se puede utilizar la opción -auto.
Deje que SnapManager gestione la copia de seguridad de una base de datos, independientemente de si está en línea o sin conexión	Especifique la opción -auto. Si se usa la opción -auto, no se puede utilizar la opción -offline o -online.
Agregar un comentario sobre la copia de seguridad	Especifique la opción -comment, seguida de la cadena de descripción.

Si desea…	Realice lo siguiente…
• Forzar la base de datos al estado en el que usted ha especificado para realizar una copia de seguridad, independientemente del estado en el que esté actualmente*	Especifique la opción -force.
Verificar la copia de seguridad en el momento de la creación	Especifique la opción -Verify.
Crear una copia de seguridad en almacenamiento secundario	Especifique la opción -Protect. • Si utiliza ONTAP y desea proteger el backup inmediatamente en el almacenamiento secundario, especifique la opción -Protect. La opción -protectnow no se puede aplicar en Clustered Data ONTAP. • Si utiliza Data ONTAP operando en 7-Mode y desea proteger el backup inmediatamente en un almacenamiento secundario, lo que anula la programación de protección de Protection Manager, especifique la opción -protectnow. • Para evitar el backup en el almacenamiento secundario, especifique la opción -noProtect. Si utiliza ONTAP y ha seleccionado la política de protección *SnapManager_CDOT_Vault* durante la creación del perfil, debe especificar la opción -snapvaultlabel. Debe proporcionar la etiqueta de SnapMirror que haya especificado en las reglas de la política de SnapMirror al configurar la relación de SnapVault como valor.
Especifique los valores de la clase de retención	Especifique la opción -retain e indique si el backup debe conservarse en función de una de las siguientes clases de retención: • -cada hora • - diariamente • -semanal • -mensual • -Unlimited Si no especifica la clase de retención, SnapManager utiliza -Hourly de forma predeterminada.

Ejemplos

El siguiente comando protege una copia de seguridad de la base de datos:

```
smo backup create -profile PAYDB -protect -retain -daily -full auto -label
full_bkup_sales
```

El siguiente comando protege inmediatamente un backup de la base de datos:

```
smo backup create -profile PAYDB -protectnow -retain -daily -full auto
-label full_bkup_sales
```

Restaurar backups protegidos a partir del almacenamiento secundario

Es posible restaurar backups protegidos desde almacenamiento secundario. No obstante, no puede restaurar backups desde el almacenamiento secundario si el backup también existe en el almacenamiento principal.

Información relacionada

El comando smo backup restore

Restaurar backups desde una ubicación alternativa

Creando especificaciones de restauración

Información general sobre restauraciones de backups protegidos

Puede elegir el método de restauración que desee utilizar para restaurar los datos de backup del almacenamiento secundario al almacenamiento primario.

En la siguiente tabla se explican los diferentes escenarios y métodos que se pueden utilizar para restaurar un backup desde el almacenamiento secundario:

Destino de restauración	Explicación
Directamente al almacenamiento primario	Devuelve los datos desde el sistema de almacenamiento secundario directamente a la ubicación original del sistema de almacenamiento principal a través de la misma red que se utilizó para proteger los datos. SnapManager utiliza el método de almacenamiento directo siempre que es posible. Este método no es posible si los datos están en un sistema de archivos en una red DE área de almacenamiento (SAN) y si se aplica alguna de las siguientes condiciones: • No se restauran otros archivos que no son de las bases de datos en el mismo sistema de archivos. • Se llevaron a cabo copias snapshot de los archivos de control y de datos de un sistema de archivos que se estaba restaurando en momentos diferentes. • El número de unidad lógica (LUN) está en un grupo de volúmenes, pero otros LUN en el mismo grupo de volúmenes no se están restaurando.
Directamente al host	Clona los datos en el sistema de almacenamiento secundario y monta los datos clonados en el host. Tras clonar y montar los datos, SnapManager los copia en su ubicación original.

Destino de restauración	Explicación
Indirectamente al almacenamiento o host	Devuelve los datos del sistema de almacenamiento secundario a una nueva ubicación del sistema primario a través de la misma red que se utilizó para proteger los datos y montar el nuevo almacenamiento en el host. Después de devolver y montar los datos, SnapManager los copia en su ubicación original. El método de almacenamiento indirecto puede requerir mucho tiempo para devolver los datos. SnapManager copia primero los datos en un volumen de desecho en el host primario antes de que SnapManager los utilice para restaurar y recuperar la base de datos. El hecho de que los datos reutilizables se eliminen automáticamente depende del protocolo utilizado. • Para SAN, SnapManager elimina los datos que se devuelven. • En el caso del almacenamiento conectado a la red (NAS), SnapManager elimina el contenido de los qtrees devueltos, pero no elimina los qtrees mismos. Para eliminar los qtrees, los administradores deben montar el volumen reutilizable y quitar los qtrees mediante el comando UNIX rmdir.

Si no puede devolver datos directamente al almacenamiento, SnapManager puede devolver los datos directamente al host o indirectamente al almacenamiento o al host. El método depende de la normativa que regule si la organización permite la conexión directamente al almacenamiento secundario o necesita que los datos se copien a través de la red de almacenamiento. Puede gestionar esta política definiendo la información de configuración en el archivo smo.config.

Información relacionada

Parámetros de configuración de SnapManager

Restaurar backups a partir del almacenamiento secundario

Es posible restaurar backups protegidos desde el almacenamiento secundario y elegir cómo desea volver a copiar los datos en el almacenamiento primario.

Se puede usar el comando backup restore con la opción -from-secondary para restaurar los datos del almacenamiento secundario. Si no especifica la opción -from-secondary, SnapManager restaura los datos desde las copias Snapshot del almacenamiento primario.

No se puede utilizar la opción -from-secondary si el backup existe en el almacenamiento primario; es necesario liberar el backup principal para que se pueda restaurar un backup del almacenamiento secundario. Si se utiliza un volumen temporal, se debe especificar el volumen con la opción -temp-volume.

Debe especificar la opción -copy-id siempre que especifique la opción -from-secondary. Si existe más de un backup en el sistema de almacenamiento secundario, la opción -copy-id se utiliza para especificar qué copia

de backup en el almacenamiento secundario se debe usar para la operación de restauración.

> Si se utiliza Data ONTAP en 7-Mode, es necesario especificar un valor válido para la opción -copy-id. Sin embargo, si utiliza Clustered Data ONTAP, la opción -copy-id no es necesaria.

Cuando se restauran datos desde un almacenamiento secundario, SnapManager intenta primero restaurar los datos directamente desde el sistema de almacenamiento secundario al sistema de almacenamiento primario (sin involucrar al host). Si SnapManager no puede realizar este tipo de restauración (por ejemplo, si los archivos no forman parte del sistema de archivos), SnapManager recuperará una restauración de copia de archivos del lado del host. SnapManager tiene dos métodos para realizar una restauración de copia de archivos en el lado del host desde el almacenamiento secundario. El método que selecciona SnapManager se configura en el archivo smo.config.

- Si restore.secondaryAccessPolicy = Direct, SnapManager clona los datos en el almacenamiento secundario, monta los datos clonados del sistema de almacenamiento secundario en el host, y después copia los datos del clon en el entorno activo.

  Esta es la directiva de acceso secundaria predeterminada.

- Si restore.secondaryAccessPolicy = indirecta, SnapManager copia primero los datos en un volumen temporal en el sistema de almacenamiento principal, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo.

  Esta política se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Las restauraciones mediante el método indirecto demorarán el doble de tiempo que el método directo porque se crean dos copias de los datos.

  a. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Restaure una base de datos completa si el backup seleccionado existe en el almacenamiento principal	Introduzca el siguiente comando: smo backup restore -profileprofile_name-labellabel-complete -recover -alllogs[-copy-idid]
Restaure una base de datos completa si el backup seleccionado no existe en el almacenamiento primario	Introduzca el siguiente comando: smo backup restore -profileprofile_name-labellabel-complete -recover -alllogs-from-secondary [-temp-volume <temp_volume>] [-copy-idid]

Ejemplo

El siguiente comando restaura un backup protegido desde el sistema de almacenamiento secundario:

```
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.
```

Clonar backups protegidos

Es posible usar SnapManager para clonar una copia de un backup que se ha protegido.

El host (seleccionado para el clon) debe tener acceso al almacenamiento secundario con el mismo protocolo de almacenamiento (por ejemplo, SAN o NAS).

Es posible usar la opción -from-secondary para especificar que se desea clonar desde el almacenamiento secundario.

Debe especificar la opción -copy-id siempre que especifique la opción -from-secondary. Si existe más de un backup en el sistema de almacenamiento secundario, la opción -copy-id se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe usar para clonar.

> Si se utiliza Data ONTAP en 7-Mode, es necesario especificar un valor válido para la opción -copy-id. Sin embargo, si utiliza Clustered Data ONTAP, la opción -copy-idOption no es necesaria.

Puede producirse un error al eliminar clones de backups protegidos en sistemas de almacenamiento secundario. Este problema se produce cuando la hora del sistema de los sistemas de almacenamiento primario y secundario no están sincronizados.

1. Cree un clon de una copia de backup protegida: smo clone create -backup-labelbackup_name -newsidnew_sid-labelclone_label-profileprofile_name-clonespecfull_path_to_clonespecfile-from-secondary -copy-idid

Ejemplo

```
smo clone create -label testdb_clone_clstest
-profile sys_db_finance -from-secondary -copy-id 3042
sys_db_finance_sept_08
```

SnapManager para Oracle usa Protection Manager para proteger un backup de base de datos

Cuando SnapManager para Oracle y Protection Manager están instalados en un host UNIX y en el servidor respectivamente, proporcionan al administrador de la base de datos SnapManager la capacidad de configurar y ejecutar backups de bases de datos Oracle basados en normativas en el almacenamiento secundario, y restaurar, si es necesario, los datos de los que se ha realizado un backup del almacenamiento secundario al primario.

En el siguiente ejemplo, un administrador de bases de datos que utiliza SnapManager, crea un perfil para un backup local en el almacenamiento primario y otro perfil para un backup protegido en el almacenamiento secundario. A continuación, este administrador de base de datos trabaja con su administrador de almacenamiento en red, que utiliza la consola de Protection Manager, para configurar un backup basado en normativas de esa base de datos, desde el almacenamiento primario al secundario.

Detalles de la base de datos de destino

Este ejemplo de protección integrada de bases de datos describe la protección de una base de datos de nóminas. En el ejemplo se utilizan los datos siguientes.

El administrador de la base de datos (DBA) de TechCo, una empresa de 3000 personas con sede en Atlanta, debe crear una copia de seguridad coherente de la base de datos de nóminas de producción, PAYDB. La estrategia de protección para realizar la backup en el almacenamiento primario y secundario requiere que el administrador de almacenamiento y el administrador de bases de datos Oracle trabajen conjuntamente para realizar backups de la base de datos Oracle tanto de forma local en el almacenamiento primario como remota, en un almacenamiento secundario en una ubicación remota.

- **Información del perfil**

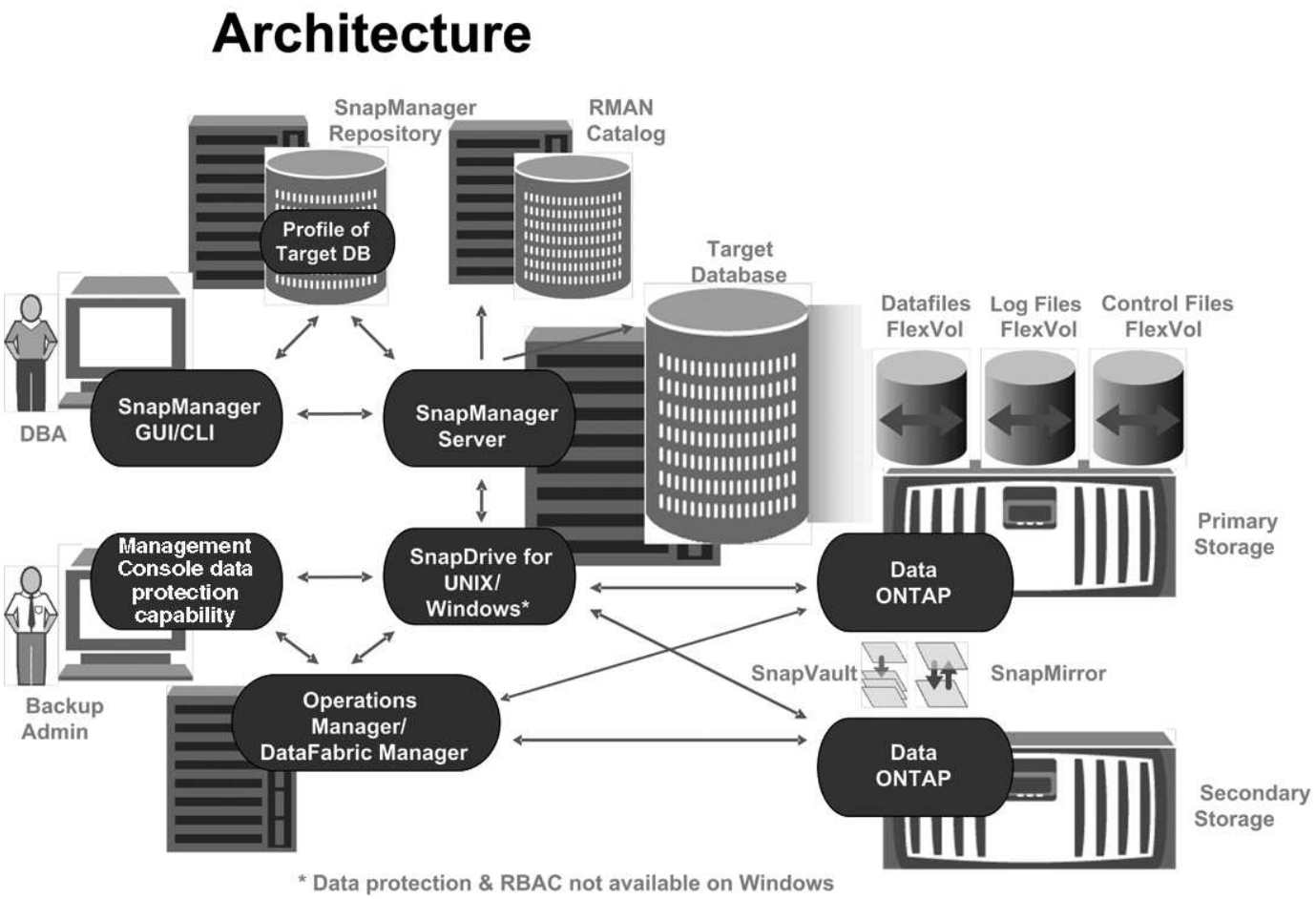
  Al crear un perfil en SnapManager, necesita los siguientes datos:

  - Nombre de la base de datos: PAYDB
  - Nombre del host: payroll.techco.com
  - ID de base de datos: Payroldb
  - Nombre del perfil: Payroll_prod
  - Modo de conexión: Autenticación de base de datos
  - Esquema de nomenclatura de Snapshot: smo_hostname_dbsid_smopirofile_scope_mode_smid (que se traduce a "smo_payroll.xyz.com_payrolldb_payroll_prod_f_h_x")

Configuración y topología de almacenamiento principal y secundario

En este ejemplo, TechCo Corporation ejecuta su base de datos de nóminas en un servidor de bases de datos que también es un host de SnapManager para Oracle y almacena los datos de su base de datos de nóminas y los archivos de configuración en los sistemas de almacenamiento primario de la sede central de la empresa. El requisito corporativo es proteger la base de datos con backups diarios y semanales en un almacenamiento local, así como backups a sistemas de almacenamiento de un sitio de almacenamiento secundario situado a 50 kilómetros de distancia.

En la siguiente ilustración, se muestran los componentes de funcionalidades de protección de datos de SnapManager para Oracle y NetApp Management Console necesarios para admitir la protección de backup local y secundario.



Para gestionar la base de datos de nóminas y respaldar su protección de copia de seguridad local y secundaria como se muestra en el gráfico anterior, se utiliza la siguiente implementación.

- **SnapManager host**

  El host SnapManager, payroll.techco.com, se encuentra en la sede de la empresa y se ejecuta en un servidor UNIX, que también ejecuta el programa de base de datos que genera y mantiene la base de datos de nóminas.

  - **Conexiones**

    Para admitir la protección de backups locales y secundarios, el host SnapManager tiene conexiones de red a los siguientes componentes:

    - SnapManager para el cliente Oracle
    - Repositorio de SnapManager, que ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
    - Sistemas de almacenamiento primario
    - Sistemas de almacenamiento secundario
    - DataFabric Manager Server
  - **Productos instalados**

    El host SnapManager se instala con los siguientes productos para este ejemplo:

        - Servidor SnapManager
        - SnapDrive para UNIX
        - Utilidades de host
- **Sistemas de almacenamiento primario TechCo**

  La base de datos de nóminas, incluidos los archivos de datos asociados, los archivos de registro y los archivos de control, residen en los sistemas de almacenamiento principales. Estas se encuentran en la sede central de la empresa TechCo, junto con el host de SnapManager y la red que conecta el almacenamiento primario con el host de SnapManager. Las últimas transacciones y actualizaciones de la base de datos de nóminas se escriben en los sistemas de almacenamiento primarios. Las copias Snapshot, que proporcionan protección mediante backup local de la base de datos de nóminas, también residen en los sistemas de almacenamiento primarios.

  - **Conexiones**

    Para admitir la protección de backups secundarios, los sistemas de almacenamiento primario tienen conexiones de red a los siguientes componentes:

    - Host SnapManager que ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
    - Sistemas de almacenamiento secundario
    - DataFabric Manager Server
  - **Productos instalados**

    Para este ejemplo, deben habilitarse las siguientes licencias en estos sistemas:

    - Data ONTAP 7.3.1 o posterior
    - ONTAP primario de SnapVaultData
    - FlexVol (necesario para NFS)
    - SnapRestore
    - Protocolo NFS
- **Sistemas de almacenamiento secundario TechCo**

  Los sistemas de almacenamiento secundario, ubicados en un sitio de almacenamiento secundario conectado a la red, a 50 km de distancia, se utilizan para almacenar backups secundarios de la base de datos de nóminas.

  - **Conexiones**

    Para admitir la protección de backup secundario, los sistemas de almacenamiento secundario tienen conexiones de red a los siguientes componentes:

    - Sistemas de almacenamiento primario
    - DataFabric Manager Server
  - **Productos instalados**

    Para este ejemplo, deben habilitarse las siguientes licencias en los sistemas de almacenamiento secundario:

        - Data ONTAP
        - SnapVaultData ONTAP secundario
        - SnapRestore
        - FlexVol (necesario para NFS)
        - Protocolo NFS
- **DataFabric Manager Server**

  DataFabric Manager Server, techco_dfm, se encuentra en la sede de la empresa en una ubicación accesible por el administrador de almacenamiento. DataFabric Manager Server, entre otras funciones, coordina las tareas de backup entre el almacenamiento principal y el secundario.

  - **Conexiones**

    Para admitir una protección de backup secundaria, DataFabric Manager Server mantiene conexiones de red con los siguientes componentes:

    - Consola de gestión de NetApp
    - Sistemas de almacenamiento primario
    - Sistemas de almacenamiento secundario
  - **Productos instalados**

    Para este ejemplo, DataFabric Manager Server cuenta con licencia para los siguientes productos de servidor:

    - DataFabric Manager
- **Repositorio de SnapManager**

  El repositorio de SnapManager, ubicado en un servidor dedicado, almacena datos sobre las operaciones realizadas por SnapManager, por ejemplo, el momento de realizar backups, los espacios de tablas y archivos de datos de los que se ha realizado backup, los sistemas de almacenamiento utilizados, los clones realizados y las copias Snapshot creadas. Cuando un administrador de base de datos intenta realizar una restauración completa o parcial, SnapManager consulta al repositorio para identificar los backups creados por SnapManager para Oracle para su restauración.

  - **Conexiones**

    Para admitir la protección de backup secundario, los sistemas de almacenamiento secundario tienen conexiones de red a los siguientes componentes:

    - Host SnapManager
    - SnapManager para el cliente Oracle
- **Consola de gestión de NetApp**

  La consola de gestión de NetApp es la consola de interfaz gráfica de usuario que utiliza el administrador de almacenamiento para configurar programaciones, políticas, conjuntos de datos y asignaciones de pools de recursos con el fin de permitir el backup en sistemas de almacenamiento secundarios, a los que el administrador de almacenamiento puede acceder.

  - **Conexiones**

Para admitir la protección de backups secundarios, NetApp Management Console tiene conexiones de red a los siguientes componentes:

  - Sistemas de almacenamiento primario
  - Sistemas de almacenamiento secundario
  - DataFabric Manager Server

- **SnapManager para el cliente Oracle**

  El cliente SnapManager para Oracle es la interfaz gráfica de usuario y la consola de línea de comandos que usa el administrador de bases de datos para la base de datos de nóminas de este ejemplo para configurar y realizar copias de seguridad locales y copias de seguridad en el almacenamiento secundario.

  - **Conexiones**

    Para admitir la protección de backups locales y secundarios, SnapManager para Oracle Client tiene conexiones de red a los siguientes componentes:

    - Host SnapManager
    - SnapManager Repository, ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
    - Host de base de datos (si está separado del host que ejecuta SnapManager)
    - DataFabric Manager Server

  - **Productos instalados**

    Para admitir la protección de copia de seguridad local y copia de seguridad secundaria, se debe instalar SnapManager para el software de cliente de Oracle en este componente.

Programa de backup y estrategia de retención

El administrador de bases de datos quiere asegurarse de que los backups estén disponibles en caso de pérdida de datos, en caso de siniestro y por motivos normativos. Esto requiere una política de retención de pensamiento detenidamente para las distintas bases de datos.

Para la base de datos de nóminas de producción, el DBA se adhiere a la siguiente estrategia de retención de TechCo:

Frecuencia de backup	Duración de la retención	El tiempo de los backups	Tipo de almacenamiento
Una vez al día	10 días	7 p. m.	Primario (local)
Una vez al día	10 días	7 p. m.	Secundario (archivado)
Una vez por semana	52 semanas	Sábados 1:00 a.m.	Secundario (archivado)

- **Ventajas de copia de seguridad local**

  El backup local diario proporciona protección de bases de datos, que es instantánea, utiliza cero ancho de

banda de red, utiliza un mínimo de espacio de almacenamiento adicional, ofrece una restauración instantánea y ofrece funciones de backup y restauración de datos muy detalladas.

Como los backups semanales finales de la base de datos de nóminas se conservan durante un mínimo de 52 semanas en un site de almacenamiento secundario, no es necesario conservar los backups diarios durante más de 10 días.

- **Ventajas de copia de seguridad protegida**

  Los backups diarios y semanales a un almacenamiento secundario en una ubicación remota garantizan que si los datos del site de almacenamiento principal presentan daños, la base de datos objetivo sigue estando protegida y podrá restaurarse a partir del almacenamiento secundario.

  Se realizan los backups diarios al almacenamiento secundario para protegerse frente a daños en el sistema de almacenamiento primario. Como los backups semanales finales de la base de datos de nóminas se conservan durante un mínimo de 52 semanas, no es necesario conservar los backups diarios durante más de 10 días.

Resumen de flujo de trabajo para backup de bases de datos local y secundario

En este ejemplo, el administrador de bases de datos (con SnapManager) y el administrador de almacenamiento (con la función de protección de datos Management Console de NetApp) coordinan las acciones para configurar los backups locales y secundarios (también conocidos como backup protegido) de la base de datos de destino.

La secuencia de acciones realizadas se resume de la siguiente manera:

- **Configuración del pool de recursos secundario**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar un conjunto de recursos de sistemas de almacenamiento en el sitio secundario que puede usarse para almacenar el backup de base de datos de nóminas.

- **Programación de copia de seguridad secundaria**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar programaciones de backup secundarias.

- **Configuración de la política de protección**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar una normativa de protección de backup secundaria para la base de datos de destino. La política de protección incluye las programaciones y especifica el tipo base de protección para implementar la protección de backups (backup, reflejo o una combinación de ambos), y nombra políticas de retención para los datos primarios, secundarios y, en ocasiones, nodos de almacenamiento terciarios.

- **Asignación de políticas de protección y configuración de perfiles de base de datos**

  El DBA utiliza SnapManager para crear o editar un perfil de la base de datos de destino que admita una copia de seguridad secundaria. Al configurar el perfil, el DBA:

  - Permite la protección de backups en el almacenamiento secundario.
  - Asigna a este perfil la nueva política de protección, que se creó en la funcionalidad de protección de

datos de NetApp Management Console y se recuperó de ella.

La asignación de la normativa de protección incluye automáticamente la base de datos de destino en un conjunto de datos parcialmente aprovisionado, pero no conforme con el conjunto de datos de la funcionalidad de protección de datos de la Consola de gestión de NetApp. Cuando está totalmente aprovisionado, la configuración del conjunto de datos permite realizar backups de la base de datos de destino en un almacenamiento secundario.

El nombre del conjunto de datos utiliza esta sintaxis: smo_hostname_datasename, que se traduce en "smo_payroll.techco.com_paydb".

- **Aprovisionamiento de almacenamiento secundario y terciario**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de Management Console de NetApp para asignar pools de recursos con el fin de aprovisionar los nodos de almacenamiento secundario y, en ocasiones, terciario (si la política de protección asignada especifica nodos de almacenamiento terciarios).

- **Backup en almacenamiento local**

  El administrador de bases de datos abre el perfil con la protección habilitada en SnapManager y crea un backup completo al almacenamiento local. El nuevo backup se muestra en SnapManager como programado para la protección, pero no protegido todavía.

- **Confirmación de copia de seguridad secundaria**

  Como el backup se basa en un perfil habilitado para la protección, el backup se transfiere al volumen secundario según la programación de la política de protección. El administrador de bases de datos utiliza SnapManager para confirmar la transferencia del backup a un almacenamiento secundario. Una vez que el backup se ha copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido".

Protección de la configuración y ejecución de backups

Es necesario configurar SnapManager y Protection Manager para admitir backups de bases de datos en el almacenamiento secundario. El administrador de la base de datos y el administrador de almacenamiento deben coordinar las acciones correspondientes.

Uso de SnapManager para Oracle para crear el perfil de base de datos para un backup local

Los administradores de bases de datos utilizan SnapManager para crear un perfil de base de datos que se utilizará para iniciar una copia de seguridad en el almacenamiento local en un sistema de almacenamiento primario. Los procesos de creación de perfiles y de creación de backups se realizan por completo en SnapManager; no implican Protection Manager.

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para las copias de seguridad. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos, en su lugar sólo se proporciona el nombre del perfil. Un perfil sólo puede hacer referencia a una base de datos. Se puede hacer referencia a esa misma base de datos por más de un perfil.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol repositorios SnapManager, haga clic con el botón secundario del ratón en el host que desee asociar a este perfil y seleccione **Crear perfil**.
3. En la página Información de configuración del perfil, introduzca la siguiente información y haga clic en **Siguiente**.
   - Nombre del perfil: Payroll_prod
   - Contraseña de perfil: Payroll123
   - Comentario: Base de datos de nóminas de producción
4. En la página Database Configuration Information (Información de configuración de la base de datos), introduzca la siguiente información y haga clic en **Next** (Siguiente).
   - Nombre de la base de datos: PAYDB
   - SID de base de datos: Payroldb
   - Host de la base de datos: Acepte el valor predeterminado

     Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.
5. En la segunda página Información de configuración de la base de datos, acepte la siguiente información de la base de datos y haga clic en **Siguiente**:
   - Cuenta de host, que representa la cuenta de usuario de Oracle: oracle
   - Host Group, que representa al grupo Oracle: dba
6. En la página Información de conexión a la base de datos, seleccione **utilizar autenticación de base de datos** para permitir que los usuarios se autentiquen mediante la información de la base de datos.

   Para este ejemplo, introduzca la siguiente información y haga clic en **Siguiente**.

   - SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
   - Contraseña (contraseña SYSDBA): oracle
   - Puerto para conectarse al host de la base de datos: 1521
7. En la página Información de configuración de RMAN, seleccione **no utilizar RMAN** y haga clic en **Siguiente**.

   Oracle Recovery Manager (RMAN) es una herramienta de Oracle que ayuda a realizar el backup y la recuperación de bases de datos de Oracle mediante la detección a nivel de bloque.

8. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables. La única variable que se requiere es la variable **smid**, que crea un identificador de instantánea único.

   Para este ejemplo, haga lo siguiente:

   a. En la lista símbolo de variable, seleccione la variable **{usertext}** y haga clic en **Agregar**.
   b. Introduzca "payroll.techco.com_" como nombre de host y haga clic en **Aceptar**.
   c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de "smo" en el cuadro Formato .

d. Haga clic en **Siguiente**.

La convención de nomenclatura de Snapshot de smo_hostname_smoprofile_dbsid_Scope_mode_smid se convierte en "smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (donde "f" indica un backup completo, la "a" indica el modo automático, y la "x" representa el SMID único).

9. En la página realizar operación, compruebe la información y haga clic en **Crear**.
10. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

Uso de Protection Manager para configurar un pool de recursos secundario

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para organizar los sistemas de almacenamiento secundario habilitados con la licencia secundaria de SnapVault en un conjunto de recursos para los backups.

Lo ideal es que los sistemas de almacenamiento de un conjunto de recursos sean intercambiables en cuanto a su aceptación como destinos para los backups. Por ejemplo, al desarrollar la estrategia de protección para la base de datos de nóminas, como administrador de almacenamiento, identificó los sistemas de almacenamiento secundarios con niveles de servicio y rendimiento similares que serían miembros adecuados del mismo conjunto de recursos.

Ya creó agregados de espacio no utilizado en sistemas de almacenamiento que piensa asignar a pools de recursos. De este modo se garantiza que haya espacio adecuado para contener las copias de seguridad.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos** > **grupos de recursos**.

   Aparecerá la ventana Pools de recursos.

3. Haga clic en **Agregar**.

   Se iniciará el asistente Add Resource Pool.

4. Complete los pasos del asistente para crear el pool de recursos **paydb_backup_resource**.

   Utilice los siguientes ajustes:

   - Nombre: Use **paydb-backup_resource**
   - Umbrales de espacio (utilice los valores predeterminados):
     - Umbrales de utilización del espacio: Activado
     - Umbral casi completo (para el conjunto de recursos): 80%
     - Umbral completo (para el conjunto de recursos): 90%

Uso de Protection Manager para configurar las programaciones de backups secundarios

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para configurar una programación de backups.

Antes de configurar la programación para las copias de seguridad secundarias, el administrador de almacenamiento consulta al partner DBA la siguiente información:

- La programación que el administrador de bases de datos desea que se sigan los backups secundarios.

  En este caso, los backups únicos diarios se realizan a las 7 p. m. Y los backups una vez semanales se realizan el sábado a las 1:00

  a. Vaya a la Consola de gestión de NetApp de Protection Manager.
  b. En la barra de menús, haga clic en **políticas** > **Protección** > **programas**.

     Se muestra la pestaña Schedules de la ventana Protection Policies.

  c. Seleccione el horario diario **Diario a las 8:00 PM** en la lista de horarios.
  d. Haga clic en **Copiar**.

     En la lista se muestra un nuevo horario diario, **copia del diario a las 8:00 PM**. Ya está seleccionado.

  e. Haga clic en **Editar**.

     La hoja de propiedades Editar horario diario se abre a la ficha Programación.

  f. Cambie el nombre del programa a **nómina diaria a las 7 PM**, actualice la descripción y, a continuación, haga clic en **aplicar**.

     Se guardan los cambios.

  g. Haga clic en la ficha **Eventos diarios**.

     La hora actual de copia de seguridad diaria de la programación es de 8:00 p.m. aparece en pantalla.

  h. Haga clic en **Agregar** e introduzca **7:00 PM** en el nuevo campo Hora y, a continuación, haga clic en **aplicar**.

     La hora actual de copia de seguridad diaria del programa es ahora a las 7:00 p.m.

  i. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

     Su nuevo horario diario, **Payroll Daily a las 7 PM**, se muestra en la lista de horarios.

  j. Seleccione el horario semanal **Domingo a las 8:00 PM más diariamente** en la lista de horarios.
  k. Haga clic en **Copiar**.

     En la lista se muestra un nuevo horario semanal, **copia del domingo a las 8:00 PM más diario**. Ya está seleccionado.

  l. Haga clic en **Editar**.

     La hoja de propiedades Editar horario semanal se abre a la ficha Programación.

  m. Cambie el nombre del programa a **Payroll Saturday a la 1 AM PLUS Daily a las 7 PM** y actualice la descripción.
  n. En la lista desplegable **Horario diario**, seleccione el horario diario que acaba de crear, **Payroll Daily a las 7 PM**.

Seleccionar **nómina diaria a las 7 PM** significa que este programa define cuándo se producen las operaciones diarias cuando se aplica a una política el programa **nómina de sábado a la 1 AM más diario a las 7 PM**.

o. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

   Su nuevo horario semanal, **Payroll Saturday a la 1 AM más diariamente a las 7 PM**, se muestra en la lista de horarios.

Uso de Protection Manager para configurar una política de protección de backups secundarios

Después de configurar la programación de backup, el administrador de almacenamiento configura una normativa de almacenamiento de backup protegido en la que se incluirá dicha programación.

Antes de configurar la normativa de protección, el administrador de almacenamiento le ofrece al partner DBA la siguiente información:

- Duración de retención que se debe especificar para el almacenamiento secundario
- Tipo de protección del almacenamiento secundario requerida

La política de protección que se crea, puede listarse en SnapManager para Oracle por parte del socio de administrador de bases de datos y asignarse a un perfil de base de datos para la protección de los datos.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **políticas** > **Protección** > **Descripción general**.

   Se muestra la pestaña Overview de la ventana Protection Policies.

3. Haga clic en **Agregar directiva** para iniciar el asistente Agregar directiva de protección.
4. Complete el asistente con los siguientes pasos:

   a. Especifique un nombre de política descriptivo.

      Para este ejemplo, introduzca **TechCo Payroll Data: Copia de seguridad** y una descripción y, a continuación, haga clic en **Siguiente**.

   b. Seleccione una política base.

      Para este ejemplo, seleccione **copia de seguridad** y haga clic en **Siguiente**.

   c. En la hoja de propiedades de la directiva del nodo de datos principal, acepte la configuración predeterminada y haga clic en **Siguiente**.

      > En este ejemplo, se aplica la programación de backup local configurada en SnapManager. Se ignora cualquier programación de backup local especificada con este método.

   d. En la hoja de propiedades de conexión de datos primarios a copia de seguridad, seleccione una programación de copia de seguridad.

      Para este ejemplo, seleccione **Payroll Saturday a la 1 AM más diariamente a las 7 PM** como su

programa de copia de seguridad y, a continuación, haga clic en **Next**.

En este ejemplo, la programación seleccionada incluye tanto las programaciones semanales como diarias que se configuraron anteriormente.

e. En la hoja de propiedades Backup policy, especifique el nombre del nodo de backup y los tiempos de retención de los backups Daily, Weekly o Monthly.

Para este ejemplo, especifique una retención de backup diaria de 10 días y una retención de backup semanal de 52 semanas. Después de completar cada hoja de propiedades, haga clic en **Siguiente**.

Una vez completadas todas las hojas de propiedades, el asistente para agregar directivas de protección muestra una hoja de resumen de la directiva de protección que desea crear.

5. Haga clic en **Finalizar** para guardar los cambios.

La política de protección de **TechCo Payroll Data: Backup** se incluye entre las demás políticas configuradas para Protection Manager.

El socio DBA puede ahora usar SnapManager para Oracle para enumerar y asignar esta política al crear el perfil de base de datos para proteger los datos.

Utilice SnapManager para Oracle para crear el perfil de base de datos y asignar una política de protección

Debe crear un perfil en SnapManager para Oracle, habilitar la protección en el perfil y asignar una política de protección para crear un backup protegido.

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para backups. Después de crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación. Un perfil sólo puede hacer referencia a una base de datos, pero es posible hacer referencia a esa misma base de datos mediante más de un perfil.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol repositorios, haga clic con el botón secundario del ratón en el host y seleccione **Crear perfil**.
3. En la página Información de configuración del perfil, introduzca los detalles del perfil y haga clic en **Siguiente**.

   Puede introducir la siguiente información:

   - Nombre del perfil: Payroll_prod2
   - Contraseña de perfil: Payroll123
   - Comentario: Base de datos de nóminas de producción
4. En las páginas Database Configuration Information (Información de configuración de la base de datos), introduzca los detalles de la base de datos y haga clic en **Next** (Siguiente).

   Puede introducir la siguiente información:

   - Nombre de la base de datos: PAYDB
   - SID de base de datos: Payroldb
   - Host de la base de datos: Acepte el valor predeterminado. Debido a que está creando un perfil a partir

de un host en el árbol de repositorios, SnapManager muestra el nombre de host.

- Cuenta de host, que representa la cuenta de usuario de Oracle: oracle
- Host Group, que representa al grupo Oracle: dba

5. En la página Información de conexión a la base de datos, haga clic en **usar autenticación de base de datos** para permitir que los usuarios autentiquen mediante información de la base de datos.
6. Introduzca los detalles de conexión de la base de datos y haga clic en **Siguiente**.

   Puede introducir la siguiente información:

   - SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
   - Contraseña (contraseña SYSDBA): oracle
   - Puerto para conectarse al host de la base de datos: 1521
7. En la página Información de configuración de RMAN, haga clic en **no utilizar RMAN** y haga clic en **Siguiente**.

   Oracle Recovery Manager (RMAN) es una herramienta de Oracle que ayuda a realizar el backup y la recuperación de bases de datos de Oracle mediante la detección a nivel de bloque.

8. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables.

   La variable smid crea un identificador de instantánea único.

   Realice lo siguiente:

   a. En la lista símbolo de variable, seleccione texto de usuario y haga clic en **Agregar**.
   b. Introduzca payroll.techco.com_ como nombre de host y haga clic en **Aceptar**.
   c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de smo en el cuadro Formato .
   d. Haga clic en **Siguiente**.

   La convención de nomenclatura de Snapshot de smo_hostname_smoprofile_dbsid_Scope_mode_smid se convierte en "smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (donde "f" indica un backup completo, "a" indica el modo automático, y "x" representa el SMID único).

9. Seleccione **Directiva de protección de Protection Manager**.

   La normativa de protección de Protection Manager le permite seleccionar una directiva de protección configurada mediante la Consola de gestión de NetApp.

10. Seleccione **TechCo Payroll Data: Backup** como política de protección de las políticas de protección recuperadas de NetApp Management Console y haga clic en **Siguiente**.
11. En la página realizar operación, compruebe la información y haga clic en **Crear**.
12. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

    - La asignación de una normativa de protección de la consola de gestión de NetApp al perfil de la base de datos crea automáticamente un conjunto de datos no conforme, visible para el operador de la consola de gestión de NetApp, con el nombre de convención smo_<hostname>_<profilename>, o en este ejemplo: smo_payroll.tech.com_PAYDB.

- Si el perfil no es apto para la restauración de volumen (también llamado "restauración rápida"), se produce lo siguiente:
  - La ficha **resultados** indica que la creación del perfil se ha realizado correctamente y que se han producido advertencias durante la operación.
  - La ficha **Detalles de operación** incluye un registro DE ADVERTENCIA, que indica que el perfil no es elegible para una restauración rápida y explica por qué.

Uso de Protection Manager para aprovisionar el nuevo conjunto de datos

Una vez creado el conjunto de datos smo_paydb, el administrador de almacenamiento usa Protection Manager para asignar recursos del sistema de almacenamiento a fin de aprovisionar el nodo de backup del conjunto de datos.

Antes de aprovisionar el conjunto de datos recién creado, el administrador de almacenamiento consulta al partner DBA el nombre del conjunto de datos especificado en el perfil.

En este caso, el nombre del conjunto de datos es smo_payroll.tech.com_PAYDB.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos** > **conjuntos de datos** > **Descripción general**.

   La pestaña Datasets de la ventana Datasets muestra una lista de conjuntos de datos que incluye el conjunto de datos que acaba de crear mediante SnapManager.

3. Localice y seleccione el conjunto de datos **smo_payroll.tech.com_PAYDB**.

   Al seleccionar este conjunto de datos, el área del gráfico muestra el conjunto de datos smo_paydb con su nodo de copia de seguridad sin aprovisionar. Su estado de conformidad se Marca como no conforme.

4. Con el conjunto de datos smo_paydb todavía resaltado, haga clic en **Editar**.

   La consola de gestión de NetApp de Protection Manager muestra la ventana Editar conjunto de datos para el conjunto de datos **smo_payroll.tech.com_PAYDB**. El panel de navegación de la ventana muestra las opciones de configuración del nodo principal del conjunto de datos, la conexión de backup y el nodo de backup.

5. En el panel de navegación, busque las opciones del nodo de copia de seguridad del conjunto de datos y seleccione **agrupaciones de aprovisionamiento/recursos**.

   La ventana Edit Dataset muestra una configuración de la política de aprovisionamiento predeterminada y una lista de pools de recursos disponibles.

6. Para este ejemplo, seleccione el pool de recursos **paydb_backup_resource** y haga clic en **>**.

   El pool de recursos seleccionado aparece en el campo "Pools de recursos para este nodo".

7. Haga clic en **Finalizar** para guardar los cambios.

Protection Manager aprovisiona automáticamente el nodo de copia de seguridad secundario con recursos del pool de recursos paydb_backup_resource.

Uso de SnapManager para Oracle para crear un backup protegido

Al crear un backup para este ejemplo, el administrador de bases de datos selecciona la creación de un backup completo, define las opciones de backup y selecciona la protección para el almacenamiento secundario. Si bien el backup se realiza inicialmente en el almacenamiento local, ya que este backup se basa en un perfil con protección habilitada, el backup se transfiere luego al almacenamiento secundario según la programación de la política de protección definida en Protection Manager.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol del repositorio de SnapManager, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos de la que desea realizar la copia de seguridad y seleccione **copia de seguridad**.

   Se iniciará el Asistente para copia de seguridad de SnapManager para Oracle.

3. Introduzca Production_Payroll como etiqueta.
4. Introduzca la nómina de producción Jan 19 backup como comentario.
5. Seleccione **Auto** como el tipo de copia de seguridad que desea crear.

   Esto permite a SnapManager determinar si se debe realizar un backup en línea o sin conexión.

6. Seleccione **Diario** o **Semanal** como la frecuencia de la copia de seguridad.
7. Para confirmar que la copia de seguridad tiene un formato válido para Oracle, marque la casilla junto a **verificar copia de seguridad**.

   Esta operación utiliza Oracle DBVerify para comprobar el formato de bloque y la estructura.

8. Para forzar el estado de la base de datos al modo apropiado (por ejemplo, de abierto a montado), seleccione **permitir inicio o cierre de la base de datos, si es necesario**, y haga clic en **Siguiente**.
9. En la página Database, Tablespaces o Datafiles to Backup, seleccione **Full Backup** y haga clic en **Next**.
10. Para proteger la copia de seguridad en almacenamiento secundario, seleccione **proteger la copia de seguridad** y haga clic en **Siguiente**.
11. En la página realizar operación, compruebe la información suministrada y haga clic en **copia de seguridad**.
12. En la página Progress, consulte el progreso y los resultados de la creación de backup.
13. Para ver los detalles de la operación, haga clic en **Detalles de la operación**.

Usar SnapManager para Oracle para confirmar la protección del backup

Con SnapManager para Oracle, se puede ver una lista de backups asociados a un perfil, determinar si los backups estaban habilitados para la protección y ver la clase de retención (diaria o semanal, en este ejemplo).

Al principio, el nuevo backup en este ejemplo se muestra como programado para la protección, pero no está protegido aún (en la interfaz gráfica de usuario de SnapManager y en el resultado del comando backup show). Una vez que el administrador de almacenamiento garantiza que el backup se haya copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido" en la interfaz gráfica de usuario y con el comando backup list.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol del repositorio de SnapManager, expanda el perfil para mostrar sus copias de seguridad.
3. Haga clic en la ficha **copias de seguridad/clones**.
4. En el panel Informes, seleccione **Detalles de copia de seguridad**.
5. Consulte la columna Protection y asegúrese de que el estado sea "Protected".

Restauración de base de datos desde backup

Si el contenido activo de la base de datos de nóminas se pierde o destruye accidentalmente, SnapManager y la función de protección de datos de la consola de gestión de NetApp permiten la restauración de esos datos desde un backup local o un almacenamiento secundario.

Uso de SnapManager para Oracle para restaurar un backup local en el almacenamiento primario

Es posible restaurar backups locales que estén en el almacenamiento principal. Todo el proceso se realiza mediante SnapManager para Oracle.

También puede obtener una vista previa de la información acerca de un proceso de restauración de copia de seguridad. Puede que desee hacer esto para ver información acerca de la elegibilidad de restauración de un backup. SnapManager analiza los datos de un backup para determinar si puede completarse el proceso de restauración usando la restauración basada en volúmenes o el método de restauración basada en archivos.

La vista previa de la restauración muestra la siguiente información:

- Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se utilizará para restaurar cada archivo.
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo.

En la vista previa del plan de restauración, SnapManager no restaura nada. La vista previa muestra información de hasta 20 archivos.

Si desea obtener una vista previa de una restauración de archivos de datos pero la base de datos no está montada, SnapManager monta la base de datos. Si no se puede montar la base de datos, la operación genera un error y SnapManager devuelve la base de datos a su estado original.

1. En el árbol del repositorio, haga clic con el botón derecho del ratón en la copia de seguridad que desea restaurar y seleccione **Restaurar**.
2. En la página de bienvenida del Asistente para restauración y recuperación, haga clic en **Siguiente**.
3. En la página Restore Configuration Information, seleccione **Complete Datafile/Tablespace Restore with Control Files**.
4. Haga clic en **permitir cierre de la base de datos si es necesario**.

   SnapManager cambia el estado de la base de datos, si es necesario. Por ejemplo, si la base de datos está sin conexión y debe estar en línea, SnapManager la fuerza a la conexión.

5. En la página Información de configuración de recuperación, haga clic en **todos los registros**.

   SnapManager restaura y recupera la base de datos a la última transacción y aplica todos los registros

requeridos.

6. En la página Restore Source Location Configuration (Restaurar configuración de ubicación de origen), consulte la información sobre la copia de seguridad en primaria y haga clic en **Next** (Siguiente).

   Si el backup solo se realiza en el almacenamiento primario, SnapManager restaura el backup desde el almacenamiento primario.

7. En la página Volume Restore Configuration Information (Información de configuración de la restauración de volumen), seleccione **intentar la restauración de volumen** para intentar el método de restauración de volumen.
8. Haga clic en **Volver a restauración basada en archivos**.

   Así, SnapManager puede utilizar el método de restauración basada en archivos si no se puede utilizar el método de restauración de volumen.

9. Haga clic en **Vista previa** para ver las comprobaciones de elegibilidad para obtener una rápida restauración e información sobre comprobaciones obligatorias y anulables.
10. En la página realizar operación, compruebe la información introducida y haga clic en **Restaurar**.
11. Para ver detalles sobre el proceso, haga clic en **Detalles de la operación**.

Uso de SnapManager para Oracle para restaurar backups desde almacenamiento secundario

Los administradores pueden restaurar backups protegidos a partir de almacenamiento secundario y elegir cómo desean copiar los datos de nuevo en el almacenamiento primario.

Antes de intentar restaurar el backup, compruebe las propiedades del backup y asegúrese de que el backup se libere en el sistema de almacenamiento principal y esté protegido en el almacenamiento secundario.

1. En el árbol del repositorio de SnapManager para Oracle, haga clic con el botón derecho del ratón en la copia de seguridad que desea restaurar y seleccione **Restaurar**.
2. En la página de bienvenida del Asistente para restauración y recuperación, haga clic en **Siguiente**.
3. En la página Restore Configuration Information, haga clic en **Complete Datafile/Tablespace Restore with Control Files**.
4. Haga clic en **permitir cierre de la base de datos si es necesario** y, a continuación, haga clic en **Siguiente**.

   SnapManager cambia el estado de la base de datos, si es necesario. Por ejemplo, si la base de datos está sin conexión y debe estar en línea, SnapManager la fuerza a la conexión.

5. En la página Información de configuración de recuperación, haga clic en **todos los registros**. A continuación, haga clic en **Siguiente**.

   SnapManager restaura y recupera la base de datos a la última transacción y aplica todos los registros requeridos.

6. En la página Restore Source Location Configuration (Restaurar configuración de ubicación de origen), seleccione el ID del origen de copia de seguridad protegida y haga clic en **Next** (Siguiente).
7. En la página Información de configuración de la restauración de volumen, haga clic en **intentar la restauración de volumen** para intentar la restauración de volumen.

8. Haga clic en **Volver a restauración basada en archivos**.

   Esto permite a SnapManager utilizar el método de restauración basada en archivos si no se puede completar el método de restauración de volúmenes.

9. Para ver las comprobaciones de elegibilidad para obtener una rápida restauración e información sobre comprobaciones obligatorias y anulables, haga clic en **Vista previa**.
10. En la página realizar operación, compruebe la información que ha proporcionado y haga clic en **Restaurar**.
11. Para ver detalles sobre el proceso, haga clic en **Detalles de la operación**.

Realizando operaciones de gestión

Es posible realizar tareas de gestión después de instalar y configurar SnapManager. Estas tareas le permiten gestionar las operaciones normales más allá del backup, la restauración y la clonación.

Los administradores pueden realizar operaciones mediante la interfaz gráfica de usuario o la interfaz de línea de comandos.

Ver una lista de operaciones

Es posible ver una lista con un resumen de todas las operaciones realizadas en un perfil.

Puede ver la siguiente información cuando enumere operaciones asociadas a un perfil en particular:

- Fecha de inicio y finalización cuando se ejecutó la operación
- Estado de la operación
- ID de la operación
- Tipo de operación
- Host en el que se ejecutó

  a. Para enumerar la información resumida de todas las operaciones, utilice el siguiente comando: `smo operation list profile -profile profile_name-delimiter character [-quiet | -verbose]`

     Cuando se especifica la opción -delimitador, el comando enumera cada fila en una línea separada y los atributos de esa fila están separados por el carácter especificado.

Información relacionada

El comando smo operation list

Ver los detalles de la operación

Puede ver información detallada acerca de un perfil determinado para verificar el éxito o el fracaso de una operación. También puede ayudar a determinar los recursos de almacenamiento que se están utilizando para una operación en particular.

Es posible ver los siguientes detalles sobre una operación en particular:

- ID de la operación
- Tipo de operación
- Si la operación se ha forzado
- Información de tiempo de ejecución, incluido el estado, la fecha de inicio y de finalización de la operación
- El host donde se ejecutó la operación, incluidos el ID de proceso y la versión de SnapManager
- Información del repositorio
- Recursos de almacenamiento en uso

  a. Para ver la información detallada de un ID de operación específico, escriba el siguiente comando: `smo operation show -profile profile_name [-label label | -id id] [-quiet | -verbose]`

Información relacionada

El comando smo operation show

Emitir comandos desde un host alternativo

Puede emitir comandos de la CLI desde un host distinto al host de la base de datos y SnapManager enrutará los comandos que introduzca al host adecuado.

Para que el sistema pueda enviar una operación al host correcto, primero debe saber dónde encontrar el perfil para la operación. En este procedimiento, el sistema mantiene el perfil en la información de asignación de repositorios para un archivo en el directorio principal del usuario en el host local.

1. Para que el directorio principal del usuario local conozca las asignaciones de perfil a repositorio de modo que pueda enrutar la solicitud de operación, introduzca el siguiente comando: `smo profile sync -repository-dbname repo_dbname-host repo_host-port repo_port-login-username repo_username [-quiet | -verbose]`

Comprobación de la versión del software SnapManager

Puede determinar qué versión del producto se ejecuta en el host local ejecutando el comando version.

1. Para comprobar la versión de SnapManager, introduzca este comando: Versión de smo

Información relacionada

El comando version de smo

Detener el servidor host SnapManager

Cuando termine de utilizar SnapManager, quizás desee detener el servidor.

1. Para detener el servidor, escriba el siguiente comando, como usuario raíz: `smo_server stop`

Información relacionada

El comando smo_Server stop

Reiniciar el servidor host UNIX de SnapManager

Puede reiniciar el servidor en un host UNIX utilizando la CLI.

1. Para reiniciar el servidor, introduzca el siguiente comando: `smo_server restart`

Desinstalar el software de un host UNIX

Si ya no necesita el software SnapManager, puede desinstalarlo desde el servidor host.

1. Inicie sesión como root.
2. Para detener el servidor, escriba el siguiente comando: `smo_server stop`
3. Para quitar el software SnapManager, introduzca el siguiente comando: `UninstallSmo`
4. Después del texto de introducción, pulse **Intro** para continuar.

   Se completa la desinstalación.

Información relacionada

El comando smo_Server stop

Configuración de una notificación por correo electrónico

SnapManager permite recibir una notificación por correo electrónico acerca del estado de finalización de las operaciones de base de datos ejecutadas por perfil. SnapManager genera el correo electrónico y ayuda a realizar la acción adecuada en función del estado de finalización de la operación de la base de datos. La configuración de las notificaciones por correo electrónico es un parámetro opcional.

Puede configurar una notificación por correo electrónico para un perfil individual como notificación de perfil y para varios perfiles en una base de datos de repositorio como notificación de resumen.

Notificación de perfiles

Para un perfil individual, es posible recibir un correo electrónico para las operaciones de base de datos correctas o fallidas.

> De forma predeterminada, la notificación por correo electrónico está habilitada para las operaciones con bases de datos fallidas.

Notificación de resumen

La notificación de resumen permite recibir un mensaje de correo electrónico resumido sobre las operaciones de la base de datos realizadas mediante varios perfiles. Se pueden habilitar notificaciones por hora, por día, por semana o por mes.

En SnapManager 3.3, las notificaciones de resumen se envían solo si se especifica el servidor host que tiene que enviar la notificación. Si se actualiza SnapManager desde una versión anterior a 3.3, es posible que las notificaciones de resumen no se envíen si no se especificó el servidor host en la configuración de notificaciones de resumen.

Si crea un repositorio en un nodo de una base de datos que se encuentra en un entorno RAC y habilita la notificación de resumen, posteriormente cuando agrega el mismo repositorio a otro nodo de la base de datos, el correo electrónico de notificación de resumen se envía dos veces.

Puede usar notificación a nivel de perfil o notificación de resumen al mismo tiempo.

SnapManager habilita la notificación por correo electrónico para las siguientes operaciones de bases de datos ejecutadas por perfiles:

- Crear backup en el almacenamiento principal
- Restaurar backups
- Crear clones
- Divida los clones
- Verificar backups

Después de crear o actualizar perfiles con la notificación de correo electrónico activada, puede desactivarla. Si deshabilita la notificación por correo electrónico, ya no recibirá alertas por correo electrónico para esas operaciones de base de datos ejecutadas por perfil.

El correo electrónico que recibe contiene los siguientes detalles:

- Nombre de la operación de base de datos, por ejemplo, backup, restauración o clonado
- Nombre de perfil utilizado para la operación de base de datos
- Nombre del servidor host
- Identificador del sistema de la base de datos
- Hora de inicio y finalización de la operación de base de datos
- Estado de la operación de base de datos
- Mensaje de error, si lo hay
- Mensajes de advertencia, si los hay

Puede configurar lo siguiente:

- Servidor de correo para un repositorio
- Notificación por correo electrónico de un nuevo perfil
- Notificación por correo electrónico de un perfil existente
- Notificación por correo electrónico de resumen para varios perfiles en un repositorio

Es posible configurar las notificaciones por correo electrónico desde la interfaz de línea de comandos (CLI) y la interfaz gráfica de usuario (GUI).

Configuración de un servidor de correo para un repositorio

SnapManager permite especificar los detalles del servidor de correo desde los cuales se envían las alertas por correo electrónico.

SnapManager permite especificar el nombre de host o la dirección IP del servidor de correo electrónico del remitente y el número de puerto del servidor de correo electrónico para un nombre de la base de datos de repositorio que requiere la notificación por correo electrónico. Puede configurar el número de puerto del servidor de correo en un intervalo comprendido entre 0 y 65535; el valor predeterminado es 25. Si requiere autenticación para la dirección de correo electrónico, puede especificar el nombre de usuario y la contraseña.

Debe especificar el nombre o la dirección IP del servidor host que maneja la notificación por correo electrónico.

1. Para configurar el servidor de correo para que envíe alertas por correo electrónico, introduzca el siguiente comando: smo notification set -sender-emailemail_address-mailhosthost-mailportmailport [-authentication-usernameusername-passwordpassword] -repository_Port-dbnamerepo_service-hostrepo_host-login -usernamerepo_username

   Las demás opciones para este comando son las siguientes:

   [-fuerza]

Para hacer lo siguiente…	Realice lo siguiente…
Para especificar la dirección de correo electrónico del remitente.	Especifique la opción -sender-email. En SnapManager 3.2 para Oracle, puede incluir guión (-) al especificar el nombre de dominio de la dirección de correo electrónico. Por ejemplo, puede especificar la dirección de correo electrónico del remitente como -sender-emailuser@org-corp.com.
Para especificar el nombre de host o la dirección IP del servidor de correo electrónico del remitente.	Especifique la opción -mailhost.
Especificar el número de puerto del servidor de correo electrónico para un nombre de base de datos de repositorio que requiere notificación por correo electrónico. Puede configurar el número de puerto del servidor de correo en un intervalo comprendido entre cero y 65535; el valor predeterminado es 25.	Especifique la opción -mailport.
Especifique el nombre de usuario y la contraseña si necesita autenticación para la dirección de correo electrónico.	Especifique la opción -Authentication seguida del nombre de usuario y la contraseña.

En el siguiente ejemplo se configura el servidor de correo.

```
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
```

Configuración de la notificación por correo electrónico para un perfil nuevo

Cuando se crea un perfil nuevo, se puede configurar para recibir una notificación por correo electrónico al finalizar la operación de la base de datos.

- Debe configurar la dirección de correo electrónico desde la cual se envían las alertas.
- Debe usar una lista separada por comas para varias direcciones de correo electrónico.

  Debe asegurarse de que no hay espacio entre la coma y la siguiente dirección de correo electrónico.

  a. Introduzca el siguiente comando: smo profile create -profileprofile [-profile-passwordprofile_password] -repository [-dbnamercompenspo_service_name-hotrepo_host_portrepo_Port-login-ususerpo [-nombreerpo-nombre_base-dbnamedb] [-nombre_nombre_host] [-did_nombre_usuario]-did-nombredeusuario] [-diserd-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario-nombredearchivo-nombredeusuario-nombredearchivo] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredearchivo] [-nombredeusuario-nombredeusuario]-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredearchivo] [-nombredeusuario-nombredeusuario-nombredearchivo]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredearchivo] [

     Las demás opciones para este comando son las siguientes:

     [-fuerza]

     > SnapManager admite hasta 1000 caracteres para las direcciones de correo electrónico.

     Cuando se crea un backup de archivos de datos y archivos de registro de archivos junto con el perfil (para crear backups de registros de archivos independientes) y se produce un error en la creación del backup de archivos de datos, la notificación por correo electrónico se envía con el backup de datos como nombre de la operación en lugar de un backup de datos y un backup de registros de archivos. Cuando la operación de backup de archivo de datos y archivo de registro de archivo se realiza correctamente, se muestra el resultado de la siguiente manera:

```
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  :
```

En el siguiente ejemplo se muestra la notificación de correo electrónico configurada al crear un nuevo perfil:

```
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}
```

Personalización del asunto del correo electrónico para un nuevo perfil

Puede personalizar el asunto del correo electrónico para el nuevo perfil cuando lo cree.

Puede personalizar el asunto del correo electrónico utilizando el patrón {profile}_{operation-name}_{dB-sid}_{dB-host}_{start-date}_{end-date}_{status} o bien introducir su propio texto.

Nombre de la variable	Descripción	Valor de ejemplo
perfil	Nombre de perfil utilizado para la operación de base de datos	PROF1
nombre-operación	Nombre de la operación de base de datos	Backup, copia de seguridad de datos, copia de seguridad de registros de datos y archivos
db-sid	SID de la base de datos	DB1
host de base de datos	Nombre del servidor host	Hosta
fecha de inicio	La hora de inicio de la operación de la base de datos en el formato mdd:hh:ss yyyy	Abril 27 21:00:45 PST 2012
fecha de finalización	Hora de finalización de la operación de la base de datos en el formato mdd:hh:ss yyyy	Abril 27 21:10:45 PST 2012
estado	Estado de la operación de base de datos	Correcto

Si no se proporciona ningún valor para las variables, SnapManager muestra el siguiente mensaje de error: Faltan valores -Subject.

1. Introduzca el siguiente comando: smo profile create -profileprofile [-profile-passwordprofile_password] -repository [-dbnamercompenspo_service_name-hotrepo_host_portrepo_Port-login-usernamerpo [-name]-directory [-nombre_nombre_usuario]-nombredehost [-did_nombre_usuario]-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredearchivo] [-nombredeusuario-

nombredeusuario]-nombredeusuario-nombredeusuario-nombredearchivo] [-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario-nombredearchivo] [-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-d.

A continuación se muestra un ejemplo que muestra el patrón del asunto del correo electrónico:

```
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}
```

Configuración de la notificación por correo electrónico para un perfil existente

Al actualizar un perfil, puede configurar para recibir una notificación por correo electrónico al finalizar la operación de la base de datos.

- Debe configurar la dirección de correo electrónico desde la cual se envían las alertas.
- Debe introducir una sola dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas.

  Puede usar una lista separada por comas para varias direcciones. Debe asegurarse de que no hay espacio entre la coma y la siguiente dirección de correo electrónico. Si lo desea, también puede añadir un asunto al correo electrónico.

  a. Introduzca el siguiente comando:patterns profile update -profileprofile [-profile-passwordprofile_password][-database-dbnombrecompensb_dbname-host dB_host [-siddb_sid] [-login -usernamedb_username-password_password-Port_host] [{-direcciónn_email]-posess]-direcciónn-email]-nombredeusuario [-posseurb]-nombredeusuario]

     La opción Success se puede utilizar para recibir una notificación únicamente sobre las operaciones de base de datos correctas y la opción Failure para recibir una notificación solo sobre las operaciones de base de datos fallidas.

Personalización del asunto del correo electrónico para un perfil existente

SnapManager le permite personalizar el patrón de asunto del correo electrónico para un perfil existente actualizando dicho perfil. Este patrón de asunto personalizado sólo es aplicable al perfil actualizado.

1. Introduzca el siguiente comando: smo profile update -profileprofile [-profile-passwordprofile_password][-database-dbnombrecompensb_dbname-host dB_host [-siddb_sid] [-login -usernamedb_username -password_password-Port_host] [{-dirección-nombredeusuario] [-nombredeusuario_archivo_archivo]]-contraseña]-archivo_archivo_correo-archivo]-archivo-archivo-archivo-archivo-archivo-archivo] [-archivo-archivo-archivo-archivo]-archivo-archivo]-archivo-archivo-archivo-archivo]-archivo-archivo-archivo]-archivo-archivo-archivo-archivo-archivo]-archivo-archivo-archivo-archivo]-archivo-archivo-archivo-archivo-

archivo]-archivo-archivo-archivo-archivo-archivo-archivo-archivo]-archivo-archivo-archivo-archivo-archivo-archivo]-archivo-archivo-archivo-archivo-archivo-archivo-archivo]-archivo-archivo-archivo-archivo-archivo-archivo-archivo [_archivo-archivo-archivo-archivo-archivo-archivo-archivo-archivo-archivo]-archivo-archivo

En el siguiente ejemplo se muestra un patrón de asunto del correo electrónico:

```
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}
```

Configuración de notificación por correo electrónico de resumen para varios perfiles

SnapManager permite configurar una notificación por correo electrónico de resumen para varios perfiles en una base de datos de repositorio.

Es posible configurar el host del servidor SnapManager como host de notificación desde el cual se envía el correo electrónico de notificación de resumen a los destinatarios. Si se cambian el nombre de host o la dirección IP del servidor SnapManager, también se puede actualizar el host de notificación.

Puede seleccionar cualquiera de las horas de programación en las que se requiera una notificación por correo electrónico:

- Hourly: Para recibir una notificación por correo electrónico cada hora
- Diario: Para recibir una notificación por correo electrónico diariamente
- Semanal: Para recibir una notificación por correo electrónico semanalmente
- Mensual: Recibir una notificación por correo electrónico mensualmente

Debe introducir una sola dirección de correo electrónico o una lista de direcciones de correo electrónico separadas por comas para recibir notificaciones de las operaciones realizadas mediante dichos perfiles. Asegúrese de que no haya espacio entre la coma y la siguiente dirección de correo electrónico cuando introduzca varias direcciones de correo electrónico.

SnapManager le permite añadir un asunto de correo electrónico personalizado utilizando las siguientes variables:

- Nombre de perfil utilizado para la operación de base de datos.
- Nombre de la base de datos
- SID de la base de datos
- Nombre del servidor host
- Hora de inicio de la operación de la base de datos en el formato yyyymmdd:hh:ss
- Hora de finalización de la operación de la base de datos en el formato yyyymmdd:hh:ss
- Estado de la operación de base de datos

Si selecciona no agregar un asunto personalizado, SnapManager muestra un mensaje de error: Falta valor -asunto.

1. Introduzca el siguiente comando: Notificación de smo update-summary-notification -repository -portrepo_Port-dbnamerepo_service_name-hstrepo_host-login-usernamerepo_username -emailmail_dirección1,email_directs2-subjectSubject-patterm-frequency {-day-profiletime_time | -1|3 -time|4|31-time|1-time|5|6-time|7-time|1-time|1-time||1-time|1-time||-time|1-time|1-time|1-time|1||1-time|1 -time|1|-time|-time|1-time|

   Las demás opciones para este comando son las siguientes:

   [-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
   ```

Adición de un nuevo perfil para resumir las notificaciones por correo electrónico

Después de configurar una notificación por correo electrónico de resumen para la base de datos de repositorio, puede agregar un nuevo perfil a la notificación de resumen utilizando el comando summary notification.

1. Escriba el siguiente comando: smo profile create -profileprofile_name [-profile-passwordprofile_password] -repository_service_name-hotrepo_portrepo_Port-login-usernamerepo [-nombre_nombre_base-dbedb_dbedb_nombre_nombre_nombre_host] *contraseña]-nombre_usuariob]-nombre_nombre_nombre_nombre_usuariob] [-nombre_nombre_nombre_nombre_usuario]-nombre_archivo]-nombre_archivo]-nombre_nombre_usuariob]]-nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_usuariob] [-nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_archivo]]]-nombre_usuariosuerd]-nombre_nombre_nombre_nombre_usuariob] [-nombre_nombre_nombre_nombre_nombre_nombre_nombre_archivo]]-nombre_nombre_nombre_nombre_nombre_nombre_nombre_usuariob]-nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre*

   Las demás opciones para este comando son las siguientes:

   [-fuerza]

Adición de un perfil existente para resumir las notificaciones por correo electrónico

SnapManager le permite añadir un perfil existente a una notificación de correo electrónico de resumen al actualizar dicho perfil.

1. Introduzca el siguiente comando: smo profile update -profileprofile_name [-profile-passwordprofile_password] -repository_service_name-hotrepo_portrepo_Port-login-usernamerepo [-nombre_base-nombredbedb_dbedb_nombre_nombre_nombre_host] [-did_did]-nombre_nombre_usuario]-did-diserb]-nombre_nombre_usuariob] [-nombre_nombre_nombre_usuariob]-nombre_nombre_usuariob]-

nombredeusuario]-nombre_nombre_nombre_nombre_usuariob]-
nombre_nombre_nombre_nombre_nombre_nombre_usuariob] [-
nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_usuariob]]-
nombre_nombre_nombre_nombre_nombre_usuariob]-
nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_archivo]]-nombre_usuariob] [-
nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_
nombre_nombre

Desactivar la notificación por correo electrónico para varios perfiles

Después de activar la notificación de resumen por correo electrónico para varios perfiles, puede desactivarlos para que ya no reciban alertas por correo electrónico.

SnapManager permite deshabilitar la notificación de resumen por correo electrónico para esas operaciones de la base de datos ejecutadas por perfil. En la interfaz de línea de comandos de SnapManager, introduzca el comando notification remove-summary para deshabilitar la notificación por correo electrónico de resumen de varios perfiles, así como el nombre de la base de datos del repositorio para la cual no se requiere notificación por correo electrónico.

1. Para deshabilitar la notificación de resumen para varios perfiles en una base de datos de repositorio, escriba el siguiente comando: SMO notification remove-summary-notification -repository-portrepo_Port -dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username

En el siguiente ejemplo se muestra la desactivación de la notificación de resumen para varios perfiles en una base de datos de repositorio:

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5
```

Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager

SnapManager para Oracle utiliza un archivo XML (lenguaje de marcado extensible) de especificación de tareas que indica las tareas previas y las tareas posteriores para las operaciones de copia de seguridad, restauración y clonado. Es posible añadir los nombres de las tareas previas y las secuencias de comandos posteriores a las tareas en el archivo XML para que las tareas se realicen antes o después de las operaciones de backup, restauración y clonado.

En SnapManager (3.1 o anterior), puede ejecutar los scripts de tareas previas y posteriores a la tarea solo para la operación de clonado. En SnapManager (3.2 o posterior) para Oracle, puede ejecutar las secuencias de comandos previas y posteriores a la tarea para las operaciones de backup, restauración y clonado.

En SnapManager (3.1 o anterior), la sección de especificación de tareas forma parte del archivo XML de especificación del clon. Desde SnapManager 3.2 para Oracle, la sección de especificación de tareas es un archivo XML independiente.

> SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.

En SnapManager (3.2 o posterior) para Oracle, debe asegurarse de que se cumplan las siguientes condiciones para que las operaciones de SnapManager se realicen correctamente:

- Para las operaciones de copia de seguridad y restauración, utilice el archivo XML de especificación de tareas.
- Para la operación de clonado, proporcione dos archivos de especificación: Un archivo XML de especificación del clon y un archivo XML de especificación de tareas.

  Si desea habilitar la actividad de tareas previas o posteriores a la tarea, también puede agregar el archivo XML de especificación de tareas.

Puede crear el archivo de especificación de la tarea mediante la interfaz gráfica de usuario (GUI) de SnapManager, la interfaz de línea de comandos (CLI) o un editor de texto. Debe utilizar una extensión .xml para el archivo con el fin de habilitar las características de edición adecuadas. Puede guardar este archivo para usarlo para operaciones de backup, restauración y clonado futuras.

El archivo XML de especificación de tareas incluye dos secciones:

- La sección de tareas previas incluye scripts que se pueden ejecutar antes de las operaciones de backup, restauración y clonado.
- La sección tareas posteriores incluye scripts que se pueden ejecutar después de las operaciones de backup, restauración y clonado.

Los valores incluidos en las secciones de tareas previas y tareas posteriores deben cumplir las siguientes directrices:

- Nombre de la tarea: El nombre de la tarea debe coincidir con el nombre del script, que se muestra cuando se ejecuta el comando plugin.sh -describe.

  > Si hay un error de coincidencia, es posible que reciba el siguiente mensaje de error: El archivo no encontrado.

- Nombre del parámetro: El nombre del parámetro debe ser una cadena que se puede utilizar como valor de variable de entorno.

  La cadena debe coincidir con el nombre del parámetro en el script personalizado, que se muestra cuando se ejecuta el comando plugin.sh -describe .

Puede crear el archivo de especificación según la estructura del siguiente archivo de especificación de tareas de ejemplo:

```
<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>
```

El archivo XML de especificación de tareas no debe contener ninguna directiva.

En la interfaz gráfica de usuario de SnapManager, es posible establecer el valor del parámetro y guardar el archivo XML. Puede utilizar la página activación de tareas del asistente Crear copia de seguridad, del asistente Restaurar o recuperación y del asistente Crear copia de seguridad, para cargar el archivo XML de especificación de tareas existente y utilizar el archivo seleccionado para la actividad de tareas previas o posteriores a la tarea.

Una tarea se puede ejecutar varias veces, ya sea con combinaciones de parámetros y valores iguales o diferentes. Por ejemplo, puede utilizar una tarea Guardar para guardar varios archivos.

SnapManager utiliza las etiquetas XML que se proporcionan en el archivo de especificación de tareas para el procesamiento previo o la actividad de posprocesamiento para las operaciones de backup, restauración y clonado, independientemente de la extensión del archivo de especificación de la tarea.

Crear scripts de tareas previas, tareas posteriores y directivas

SnapManager le permite crear los scripts para la actividad de procesamiento previo, la actividad de procesamiento posterior y las tareas de políticas de las operaciones de backup, restauración y clonado. Debe colocar los scripts en el directorio de instalación correcto para ejecutar la actividad de preprocesamiento, la actividad de posprocesamiento y las tareas de política de la operación de SnapManager.

Contenido de secuencias de comandos de tareas previas y posteriores

Todos los scripts deben incluir lo siguiente:

- Operaciones específicas (comprobación, descripción y ejecución)
- (Opcional) variables de entorno predefinidas
- Código de manejo de errores específico (código de retorno (rc))

> Debe incluir el código de gestión de errores correcto para validar el script.

Puede utilizar los scripts de tareas previas para muchos fines, por ejemplo, limpiar un espacio en disco antes de que se inicie la operación SnapManager. También puede utilizar los scripts posteriores a la tarea, por ejemplo, para calcular si SnapManager tiene espacio en disco suficiente para completar la operación.

Contenido de secuencias de comandos de tareas de directiva

Puede ejecutar el script de directivas sin utilizar operaciones específicas como comprobar, describir y ejecutar. El script incluye las variables de entorno predefinidas (opcionales) y el código de gestión de errores específico.

El script de política se ejecuta antes de las operaciones de backup, restauración y clonado.

Formato admitido

Se puede usar un archivo de script de shell con extensión .sh como script previo y posterior.

Guía de instalación de script

El directorio en el que se instala la secuencia de comandos afecta al modo en que se utiliza. Es posible colocar los scripts en el directorio y ejecutar el script antes o después de que se lleve a cabo la operación de backup, restauración o clonado. Debe colocar el script en el directorio especificado en la tabla y utilizarlo de forma opcional al especificar la operación de backup, restauración o clonado.

> Debe asegurarse de que el directorio plugins tenga el permiso ejecutable antes de utilizar los scripts para la operación SnapManager.

Actividad	Backup	Restaurar	Clonar
Preprocesamiento	<default_installation_directory>/plugins/backup/crear/pre	<default_installation_directory>/plugins/restore/create/pre	<default_installation_directory>/plugins/clone/create/pre
Procesamiento posterior	<default_installation_directory>/ plugins/backup/creación/publicación	<default_installation_directory>/plugins/restore/create/post	<default_installation_directory>/plugins/clone/create/post
Basado en políticas	<default_installation_directory>/plugins/backup/creación/política	<default_installation_directory>/plugins/restore/create/policy	<default_installation_directory>/plugins/clone/create/policy

Ubicación de secuencias de comandos de ejemplo

A continuación se muestran algunos ejemplos de los scripts de tareas previas y posteriores a las tareas para

las operaciones de backup y clonado disponibles en la ruta de acceso del directorio de instalación:

- <default_installation_directory>/plugins/ejemplos/backup/create/pre
- <default_installation_directory>/plugins/ejemplos/backup/creación/publicación
- <default_installation_directory>/plugins/ejemplos/clon/creación/previo
- <default_installation_directory>/plugins/ejemplos/clon/creación/publicación

Qué puede cambiar en el script

Si crea un nuevo script, sólo puede cambiar las operaciones describir y ejecutar. Cada script debe contener las siguientes variables: Contexto, tiempo de espera y parámetro.

Las variables descritas en la función describir del script deben declararse al inicio del script. Puede agregar nuevos valores de parámetro en Parameter=() y utilizar los parámetros en la función EXECUTE.

Guión de muestra

A continuación se muestra un script de ejemplo con un código de retorno especificado por el usuario para calcular el espacio en el host SnapManager:

```
    #!/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
```

Operaciones en scripts de tareas

Las secuencias de comandos de tareas previas o posteriores a las tareas que cree deben seguir una estructura estándar del complemento SnapManager para Oracle.

Las secuencias de comandos de tareas previas y posteriores deben incluir las siguientes operaciones:

- comprobar
- describa
- ejecución

Si alguna de estas operaciones no se especifica en la secuencia de comandos de tareas previas o posteriores, la secuencia de comandos no será válida.

Cuando se ejecuta el comando smo plugin check para los scripts de tareas previas o posteriores, el estado devuelto de los scripts muestra un error (porque el valor de estado devuelto no es cero).

Funcionamiento	Descripción
comprobar	El servidor SnapManager ejecuta el comando plugin.sh -check para garantizar que el sistema tiene permiso de ejecución en los scripts de plugins. También es posible incluir la comprobación de permisos de archivos en el sistema remoto.

Funcionamiento	Descripción

describa	El servidor SnapManager ejecuta el comando plugin.sh -describe para obtener información acerca del script y hacer coincidir los elementos proporcionados por el archivo de especificación. El script de un plugin debe contener la siguiente información de descripción:
	
	• SM_PI_NAME: Nombre de script. Debe introducir un valor para este parámetro.
	• SM_PI_DESCRIPTION: Descripción del propósito del script. Debe introducir un valor para este parámetro.
	• SM_PI_CONTEXT: Contexto en el que se debe ejecutar el script, por ejemplo, root u oracle. Debe introducir un valor para este parámetro.
	• SM_PI_TIMEOUT: El tiempo máximo (en milisegundos) que SnapManager debe esperar a que el script complete el procesamiento y finalice la ejecución. Debe introducir un valor para este parámetro.
	• SM_PI_PARAMETER: Uno o varios parámetros personalizados necesarios para que el script del plugin realice el procesamiento. Cada parámetro debe aparecer en una nueva línea de salida e incluir el nombre del parámetro y una descripción. Cuando el script finalice el procesamiento, una variable de entorno proporcionará al script el valor del parámetro.
	
	A continuación se muestra la salida de ejemplo de la secuencia de comandos Followup_Activities.
	
	`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.`

Funcionamiento	Descripción
ejecución	El servidor SnapManager ejecuta el comando plugin.sh -execute para iniciar el script y ejecutar el script.

Información relacionada

El comando smo plugin check

Variables disponibles en los scripts de tareas para la operación de backup

SnapManager proporciona información de contexto en forma de variables de entorno relacionadas con la operación de backup que se realiza. Por ejemplo, el script puede recuperar el nombre del host original, el nombre de la política de retención y la etiqueta del backup.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
SM_OPERATION_ID	Especifica el ID de la operación actual	cadena
SM_PROFILE_NAME	Especifica el nombre del perfil utilizado	cadena
SM_SID	Especifica el identificador del sistema de la base de datos	cadena
SM_HOST	Especifica el nombre de host de la base de datos	cadena
SM_OS_USER	Especifica el propietario del sistema operativo (SO) de la base de datos	cadena
SM_OS_GROUP	Especifica el grupo del sistema operativo de la base de datos	cadena
SM_BACKUP_TYPE	Especifica el tipo de backup (en línea, sin conexión o automático)	cadena
SM_BACKUP_LABEL	Especifica la etiqueta del backup	cadena
SM_BACKUP_ID	Especifica el ID del backup	cadena
SM_BACKUP_RETENCIÓN	Especifica el período de retención	cadena

Variables	Descripción	Formato
SM_BACKUP_PROFILE	Especifica el perfil utilizado para esta copia de seguridad	cadena
SM_ALLOW_DATABASE_SHUTDOWN	Especifica si desea iniciar o cerrar la base de datos Si es necesario puede utilizar la opción -force de la interfaz de línea de comandos.	booleano
SM_BACKUP_SCOPE	Especifica el ámbito del backup (completo o parcial)	cadena
PROTECCIÓN_BACKUP_SM	Especifica si la protección de backup está habilitada	booleano
SM_TARGET_FILER_NAME	Especifica el nombre del sistema de almacenamiento de destino **Nota:** Si se utiliza más de un sistema de almacenamiento, los nombres de los sistemas de almacenamiento deben separarse con comas.	cadena
SM_TARGET_VOLUME_NAME	Especifica el nombre del volumen de destino **Nota:** el nombre del volumen de destino debe ser prefijado con el nombre del dispositivo de almacenamiento, por ejemplo, SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	cadena
SM_HOST_FILE_SYSTEM	Especifica el sistema de archivos del host	cadena
SM_SNAPSHOT_NAMES	Especifica la lista de instantáneas **Nota:** el nombre de las copias snapshot debe prefijarse con el nombre del sistema de almacenamiento y el nombre del volumen. Los nombres de las copias Snapshot están separados por comas.	matriz de cadenas
SM_ASM_DISK_GROUPS	Especifica la lista de grupos de discos de ASM	matriz de cadenas

Variables	Descripción	Formato
SM_ARCHIVE_LOGS_DIRECTORY	Especifica el directorio de registros de archivos **Nota:** Si los registros de archivos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
SM_REDO_LOGS_DIRECTORY	Especifica el directorio de redo logs **Nota:** Si los redo logs se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_SM_CONTROL	Especifica el directorio de archivos de control **Nota:** Si los archivos de control se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_DATOS_SM	Especifica el directorio de archivos de datos **Nota:** Si los archivos de datos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
definido por el usuario	Especifica parámetros adicionales definidos por el usuario. Los parámetros definidos por el usuario no están disponibles para los plugins que se usan como políticas.	definido por el usuario

Variables disponibles en los scripts de tareas para la operación de restauración

SnapManager proporciona información de contexto en la forma de variables de entorno relacionadas con la operación de restauración que se está realizando. Por ejemplo, el script puede recuperar el nombre del host original y la etiqueta del backup que se restaura.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
SM_OPERATION_ID	Especifica el ID de la operación actual	cadena
SM_PROFILE_NAME	Especifica el nombre del perfil utilizado	cadena

Variables	Descripción	Formato
SM_HOST	Especifica el nombre de host de la base de datos	cadena
SM_OS_USER	Especifica el propietario del sistema operativo (SO) de la base de datos	cadena
SM_OS_GROUP	Especifica el grupo del sistema operativo de la base de datos	cadena
SM_BACKUP_TYPE	Especifica el tipo de backup (en línea, sin conexión o automático)	cadena
SM_BACKUP_LABEL	Especifica la etiqueta de backup	cadena
SM_BACKUP_ID	Especifica el ID del backup	cadena
SM_BACKUP_PROFILE	Especifica el perfil utilizado para el backup	cadena
SM_RECOVERY_TYPE	Especifica la información de configuración de recuperación	cadena
SM_VOLUME_RESTORE_MODE	Especifica la configuración de restauración de volúmenes	cadena
SM_TARGET_FILER_NAME	Especifica el nombre del sistema de almacenamiento de destino **Nota:** Si se utiliza más de un sistema de almacenamiento, los nombres de los sistemas de almacenamiento deben separarse con comas.	cadena
SM_TARGET_VOLUME_NAME	Especifica el nombre del volumen de destino **Nota:** el nombre del volumen de destino debe ser prefijado con el nombre del dispositivo de almacenamiento, por ejemplo, SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	cadena
SM_HOST_FILE_SYSTEM	Especifica el sistema de archivos del host	cadena

Variables	Descripción	Formato
SM_SNAPSHOT_NAMES	Especifica la lista de instantáneas **Nota:** el nombre de las copias snapshot debe prefijarse con el nombre del sistema de almacenamiento y el nombre del volumen. Los nombres de las copias Snapshot están separados por comas.	matriz de cadenas
SM_ASM_DISK_GROUPS	Especifica la lista de grupos de discos de ASM	matriz de cadenas
SM_ARCHIVE_LOGS_DIRECTORY	Especifica el directorio de registros de archivos **Nota:** Si los registros de archivos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
SM_REDO_LOGS_DIRECTORY	Especifica el directorio de redo logs **Nota:** Si los redo logs se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_SM_CONTROL	Especifica el directorio de archivos de control **Nota:** Si los archivos de control se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_DATOS_SM	Especifica el directorio de archivos de datos **Nota:** Si los archivos de datos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas

Variables disponibles en los scripts de tareas para la operación de clonado

SnapManager proporciona información de contexto en forma de variables de entorno relacionadas con la operación de clonado que se realiza. Por ejemplo, el script puede recuperar el nombre del host original, el nombre de la base de datos clonada y la etiqueta del backup.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
SM_ORIGINAL_SID	SID de la base de datos original	cadena
SM_ORIGINAL_HOST	Nombre de host asociado con la base de datos original	cadena
SM_ORIGINAL_OS_USER	Propietario del sistema operativo de la base de datos original	cadena
SM_ORIGINAL_OS_GROUP	Grupo del sistema operativo de la base de datos original	cadena
SM_TARGET_SID	SID de la base de datos del clon	cadena
SM_TARGET_HOST	Nombre del host asociado con la base de datos del clon	cadena
SM_TARGET_OS_USER	Propietario del sistema operativo de la base de datos clonada	cadena
SM_TARGET_OS_GROUP	Grupo del sistema operativo de la base de datos clonada	cadena
SM_TARGET_DB_PORT	Puerto de la base de datos de destino	entero
SM_TARGET_GLOBAL_DB_NAME	Nombre de la base de datos global de la base de datos de destino	cadena
SM_BACKUP_LABEL	Etiqueta del backup utilizado para el clon	cadena

Error al manejar en scripts personalizados

SnapManager procesa la secuencia de comandos personalizada según los códigos de retorno específicos. Por ejemplo, si el script personalizado devuelve el valor 0, 1, 2 o 3, SnapManager continúa con el proceso de clonado. El código de retorno también influye en el modo en que SnapManager procesa y devuelve la salida estándar de la ejecución de la secuencia de comandos.

Código de retorno	Descripción	Continúe procesando la operación
0	El script se ha completado correctamente.	Sí

Código de retorno	Descripción	Continúe procesando la operación
1	El script se ha completado correctamente, con mensajes informativos.	Sí
2	La secuencia de comandos se ha completado, pero incluye advertencias	Sí
3	La secuencia de comandos falla, pero la operación continúa.	Sí
4 o >4	El script falla y la operación se detiene.	No

Ver scripts de plugin de muestra

SnapManager incluye scripts que puede utilizar como ejemplos para crear sus propios scripts o como base para sus scripts personalizados.

Puede encontrar los scripts de plugins de muestra en la siguiente ubicación:

- <default_install_directory>/plugins/ejemplos/backup/create
- <default_install_directory>/plugins/ejemplos/clon/crear
- <default_install_directory>/plugins/unix/examples/backup/create/post

El directorio que contiene los scripts de plug-in de ejemplo incluye los siguientes subdirectorios:

- Policy: Contiene scripts que, cuando se configuran, ejecutan siempre en la operación de clonado.
- Pre: Contiene scripts que, cuando se configuran, se ejecutan antes de la operación de clonado.
- Post: Contiene scripts que, cuando se configuran, se ejecutan después de la operación de clonado.

En la siguiente tabla se describen los scripts de ejemplo:

Nombre de script	Descripción	Tipo de script
validate_sid.sh	Contiene comprobaciones adicionales al SID utilizado en el sistema de destino. La secuencia de comandos comprueba que el SID tenga las siguientes características: • Contiene tres caracteres alfanuméricos • Comienza con una letra	Política

Nombre de script	Descripción	Tipo de script
cleanup.sh	Borra el sistema de destino de modo que esté listo para almacenar el clon recién creado. Conserva o elimina archivos y directorios en función de la necesidad.	Pretask
Mirror_the_backup.sh	Refleja los volúmenes después de que la operación de backup se produzca en un entorno UNIX cuando se utiliza Data ONTAP en 7-Mode o Clustered Data ONTAP.	Postarea
Vault_the_backup_cDOT.sh	Almacena el backup después de que se produzca la operación de backup en un entorno UNIX cuando utiliza Clustered Data ONTAP.	Postarea

Los scripts suministrados con SnapManager utilizan el shell BASH de forma predeterminada. Debe asegurarse de que el soporte para el shell BASH está instalado en su sistema operativo antes de intentar ejecutar cualquiera de los scripts de ejemplo.

1. Para verificar que está utilizando el shell BASH, introduzca el siguiente comando en el símbolo del sistema: `bash`

   Si no ve un error, el shell BASH está funcionando correctamente.

   De forma alternativa, puede introducir el comando qu-bash en el símbolo del sistema.

2. Busque el script en el siguiente directorio:

   <installdir>/plugins/ejemplos/clon/crear

3. Abra el script en un editor de secuencia de comandos como vi.

Guión de muestra

El siguiente script personalizado de muestra valida los nombres de SID de base de datos y evita que los nombres no válidos se usen en la base de datos clonada. Incluye tres operaciones (comprobación, descripción y ejecución), a las que se llama después de ejecutar el script. La secuencia de comandos también incluye el manejo de mensajes de error con los códigos 0, 4 y >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
```

Creación de scripts de tareas

Es posible crear los scripts de tareas previas, posteriores a tareas y de políticas para operaciones de backup, restauración y clonado, escribir el script e incluir las variables de entorno predefinidas en los parámetros. Es posible crear un nuevo script o modificar uno de los scripts de ejemplo de SnapManager.

Antes de comenzar a crear el script, asegúrese de lo siguiente:

- Es necesario estructurar el script de un modo determinado para que se ejecute en el contexto de una operación SnapManager.
- Debe crear el script en función de las operaciones esperadas, los parámetros de entrada disponibles y las convenciones de código de devolución.
- Debe incluir mensajes de registro y redirigir los mensajes a archivos de registro definidos por el usuario.

  a. Cree la secuencia de comandos de la tarea personalizando la secuencia de comandos de ejemplo.

     Realice lo siguiente:

     i. Busque un script de ejemplo en el siguiente directorio de instalación:

        <default_install_directory>/plugins/ejemplos/backup/create

<default_install_directory>/plugins/ejemplos/clon/crear

i. Abra el script en el editor de secuencia de comandos.
ii. Guarde el script con un nombre diferente.

b. Modifique las funciones, variables y parámetros según sea necesario.
c. Guarde el script en uno de los siguientes directorios:

Secuencias de comandos de operaciones de copia de seguridad

- <default_install_directory>/plugins/backup/create/pre: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>/plugins/backup/create/post: Ejecuta el script después de que se realiza la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>/plugins/backup/create/policy: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio. **Restaurar secuencias de comandos de operación**
- <default_install_directory>/plugins/restore/create/pre: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>/plugins/restore/create/post: Ejecuta el script después de que se realiza la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>/plugins/restore/create/policy: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio. **Clonar secuencias de comandos**
- <default_install_directory>/plugins/clone/create/pre: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>/plugins/clone/create/post: Ejecuta el script después de que se produzca la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>/plugins/clone/create/policy: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio.

Almacenamiento de los scripts de tareas

Debe almacenar los scripts de tareas previas, posteriores a tareas y de políticas en un directorio especificado en el servidor de destino donde se crearán los backups o clones. Para la operación de restauración, los scripts deben colocarse en el directorio especificado en el servidor de destino donde se desea restaurar el backup.

1. Cree el script.
2. Guarde el script en una de las siguientes ubicaciones:

Para la operación de copia de seguridad

Directorio	Descripción
<default_install_directory >/plugins/backup/crear/política	Los scripts de políticas se ejecutan antes de las operaciones de backup.

Directorio	Descripción
<default_install_directory >/plugins/backup/crear/pre	Los scripts de preprocesamiento ejecutan el antes de las operaciones de backup.
<default_install_directory >/plugins/backup/crear/post	Los scripts de procesamiento posterior se ejecutan después de las operaciones de backup.

Para la operación de restauración

Directorio	Descripción
<default_install_directory >/plugins/restore/create/policy	Los scripts de políticas se ejecutan antes de las operaciones de restauración.
<default_install_directory >/plugins/restore/create/pre	Las secuencias de comandos de preprocesamiento se ejecutan antes de las operaciones de restauración.
<default_install_directory >/plugins/restore/create/post	Los scripts posteriores al procesamiento se ejecutan después de las operaciones de restauración.

Para la operación de clonación

Directorio	Descripción
<default_install_directory >/plugins/clone/create/policy	Los scripts de políticas se ejecutan antes de las operaciones de clonado.
<default_install_directory >/plugins/clone/create/pre	Los scripts de procesamiento previo se ejecutan antes de las operaciones de clonado.
<default_install_directory >/plugins/clone/create/post	Los scripts de procesamiento posterior se ejecutan después de las operaciones de clonado.

Verificar la instalación de los scripts de los plugins

SnapManager le permite instalar y utilizar scripts personalizados para realizar diversas operaciones. SnapManager proporciona plugins para las operaciones de backup, restauración y clonado, que puede usar para automatizar sus scripts personalizados antes y después de las operaciones de backup, restauración y clonado.

1. Introduzca el siguiente comando:

   comprobación del complemento de smo -osaccount nombre de usuario de la base de datos del sistema operativo

Si no se proporciona la opción -osaccount, la verificación de la instalación del script de plugin tiene lugar para el usuario raíz en lugar de para el usuario especificado.

El siguiente resultado indica que las secuencias de comandos policy 1, pre-plugin1 y pre-plugin2 se han instalado correctamente. Sin embargo, la secuencia de comandos post-plugin1 no funciona.

```
            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.
```

Creación de un archivo de especificación de tareas

Puede crear los archivos de especificación de tareas mediante la interfaz gráfica de usuario (GUI), la interfaz de línea de comandos (CLI) o un editor de texto. Estos archivos se utilizan para realizar un procesamiento previo o la actividad de posprocesamiento de las operaciones de backup, restauración o clonado.

1. Cree un archivo de especificación de tareas mediante GUI, CLI o un editor de texto.

   Puede crear el archivo de especificación según la estructura del siguiente archivo de especificación de tareas de ejemplo:

```
<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. Introduzca el nombre del script.
3. Introduzca el nombre del parámetro y el valor asignado al parámetro.
4. Guarde el archivo XML en el directorio de instalación correcto.

Ejemplo de especificación de tarea

```
  <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>
```

Realizar operaciones de backup, restauración y clonado mediante scripts previos y posteriores

Puede usar su propio script para iniciar una operación de backup, restauración o clonado. SnapManager muestra una página Task-abling en el asistente Backup Create, el asistente Restore or Recover o el asistente Clone Create, donde puede seleccionar el script y proporcionar valores a los parámetros que requiera el script.

- Instale los scripts de los plugins en la ubicación correcta de instalación de SnapManager.
- Verifique que los plugins se hayan instalado correctamente mediante el comando smo plugin check.

- Asegúrese de que está utilizando el shell BASH.

En la interfaz de línea de comandos (CLI), enumere el nombre del script, seleccione los parámetros y configure los valores.

1. Para verificar que está usando el shell BASH, introduzca el siguiente comando en el símbolo del sistema:bash

   Como alternativa, puede introducir el comando cuál-bash en el símbolo del sistema y utilizar el resultado del comando como parámetro de inicio del script.

   El shell BASH funciona correctamente si no ve un error.

2. Para la operación de backup, introduzca la opción -taskspec y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un preprocesamiento o una actividad de posprocesamiento que se debe realizar antes o después de la operación de backup: smo backup create -profile_name {[-full {-online | -offline | -auto} [-retenga {-hora | [-diaria | -semanal | -mensual | -unlimited}] [-verify] | [-data [-lablothora archivos [archivos] | [-tablespaces [-commentation]] [-compointing] | -retain] [-Protect | -noProtect | -protectnoow] [-backup-destinpath1 [,[path2]]] [-exclude-destinpath1 [,path2]] [-pruns {-all | -untilSCNuntilSCN | -before {-dateyyyy-MM-HH:mm:ss | -desprune_copias de seguridad_en línea] [-prune]-prune-prune] -days] -topick-prune |-prune |-prune-prune-prune]-prune

   Si se produce un error en la operación del plugin de backup, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

3. Para la operación de restauración de backup, Entre en la opción -taskspec y proporcione la ruta absoluta del archivo XML de especificación de la tarea para realizar un preprocesamiento o una actividad de post-procesamiento que ocurra antes o después de la operación de restauración:smo backup restore -profileprofile_name {-<label> | -<id> <until>} {-restoreprofile|-<tablespaces> | -complete | -restauranted <files> <restorespec>} [-nallControllesologs] | {}-restoreup | { -desde-secundario [-temp-volume <temp_volume>] [-copy-idid][-taske5ry <taskspec>] [-verify][-force] backup restore -fast [require | override | fallback | off] [-preview] -dump [-quiet | -verbose]

   Si se produce un error en la operación del plugin de restauración, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

4. Para la operación de creación de clones, introduzca la opción -taskspec y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un procesamiento previo o una actividad de procesamiento posterior que debe tener lugar antes o después de la operación de clonado: clone create -profileprofile_name {-backup-labelbackup_name | -backup-<backup-id>| -current} -newsidnew_sid -clonespecefull_path_to_clonespecepecefile [-<yes, no, inherit>] [-<host>] [-<label>] [-<comment>]-deed-<id>-secondary] [-<taskspec>--poverbowed]

   Si se produce un error en la operación del plugin de clonado, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

Ejemplo de creación de una copia de seguridad utilizando el archivo XML de especificación de tareas

```
smo backup create -profile SALES1 -full -online -taskspec
sales1_taskspec.xml -force -verify
```

Actualizar el nombre del sistema de almacenamiento y el nombre de host de la base de datos de destino asociados con un perfil

Con SnapManager 3.3 o versiones posteriores, es posible actualizar el nombre de host del sistema de almacenamiento o la dirección del sistema de almacenamiento, así como el nombre de host de la base de datos de destino asociado con un perfil de SnapManager.

Actualizar el nombre del sistema de almacenamiento asociado con un perfil

A partir de la versión 3.3 de SnapManager, es posible actualizar el nombre de host o la dirección IP de un sistema de almacenamiento asociado con un perfil.

Debe asegurarse de lo siguiente:

- El perfil tiene al menos una copia de seguridad.

  Si el perfil no tiene backup, no es necesario actualizar el nombre del sistema de almacenamiento para ese perfil.

- No se está ejecutando ninguna operación para el perfil.

Puede actualizar el nombre o la dirección IP del sistema de almacenamiento mediante la interfaz de línea de comandos (CLI) de SnapManager. Mientras se actualiza el nombre del sistema de almacenamiento, se actualizan los metadatos almacenados únicamente en la base de datos del repositorio. Después de cambiar el nombre del sistema de almacenamiento, puede realizar todas las operaciones de SnapManager como antes.

> No se puede cambiar el nombre del sistema de almacenamiento mediante la interfaz gráfica de usuario (GUI) de SnapManager.

Debe asegurarse de que haya copias Snapshot disponibles en el nuevo sistema de almacenamiento. SnapManager no verifica la existencia de las copias Snapshot en el sistema de almacenamiento.

Sin embargo, debe recordar lo siguiente al realizar la actualización y reversión del host después de cambiar el nombre del sistema de almacenamiento:

- Si va a realizar una actualización gradual del host después de cambiar el nombre del sistema de almacenamiento, debe actualizar el perfil con el nuevo nombre del sistema de almacenamiento.

  Consulte *solución de problemas con los problemas de nombre del sistema de almacenamiento* para obtener información sobre cómo usar los comandos de la SnapDrive para cambiar el nombre del sistema de almacenamiento.

- Si va a revertir el host después de cambiar el nombre del sistema de almacenamiento, debe asegurarse de cambiar el nombre del sistema de almacenamiento a su nombre anterior para poder utilizar los perfiles,

los backups y los clones del sistema de almacenamiento anterior para ejecutar operaciones de SnapManager.

> Si SnapDrive no pudo identificar el sistema de almacenamiento y muestra mensajes de error, puede introducir el comando ipmigrate con los nombres de host anteriores y posteriores del sistema de almacenamiento. Para obtener información adicional sobre problemas de nombres del sistema de almacenamiento, consulte *Troubleshooting Storage system name ediciones*.

1. Introduzca el siguiente comando: `smo storage rename -profileprofile -oldnameold_storage_name-newnamenew_storage_name [quiet | -verbose]`

Si desea…	Realice lo siguiente…
Actualice el nombre del sistema de almacenamiento asociado a un perfil	Especifique la opción -profile.
Actualice el nombre o la dirección IP del sistema de almacenamiento asociados a un perfil	Especifique las siguientes opciones y variables: • -Oldnamedold_Storage_name es el nombre de host o la dirección IP del sistema de almacenamiento. • -Newnamenew_Storage_name es el nombre de host o la dirección IP del sistema de almacenamiento.

En el ejemplo siguiente se muestra el nombre del sistema de almacenamiento que se está actualizando:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Información relacionada

Solucionar problemas de cambio de nombre del sistema de almacenamiento

Ver una lista de sistemas de almacenamiento asociados a un perfil

Puede ver una lista de los sistemas de almacenamiento asociados con un perfil en particular.

La lista muestra los nombres de los sistemas de almacenamiento asociados con el perfil en particular.

> Si no hay backups disponibles para el perfil, no puede ver el nombre del sistema de almacenamiento asociado con el perfil.

1. Para mostrar información sobre los sistemas de almacenamiento asociados con un perfil determinado, escriba este comando: `smo storage list -profileprofile [-quiet | -verbose]`

Ejemplo

```
smo storage list -profile mjubllian
```

```
Sample Output:
Storage Controllers
--------------------
STCO1110-RTP07OLD
```

Actualizar el nombre de host de la base de datos de destino asociado a un perfil

SnapManager (3.2 o posterior) para Oracle ofrece la posibilidad de actualizar el nombre de host de la base de datos de destino en el perfil de SnapManager.

- El directorio inicial del usuario local debe tener en cuenta las asignaciones de perfil a repositorio.
- Se deben cerrar las sesiones de la interfaz gráfica de usuario (GUI) de SnapManager.
- En un entorno RAC, los clones o backups montados disponibles en el host especificado en el perfil deben eliminarse y desmontarse.

Puede actualizar el perfil con el nuevo nombre de host únicamente mediante la CLI.

Escenarios no admitidos para cambiar el nombre de host de la base de datos de destino en Profile

Las siguientes situaciones no son compatibles para cambiar el nombre de host de la base de datos de destino en el perfil:

- Cambiar el nombre de host de la base de datos de destino mediante la interfaz gráfica de usuario de SnapManager
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil
- Actualizar varios perfiles para un nuevo nombre de host de base de datos de destino ejecutando un solo comando
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager
- Cambiar el nombre de host de la base de datos de destino si SnapManager se instala en Solaris y si los números de unidad lógica de base de datos (LUN) se crean mediante el sistema de archivos montado en host con la pila de SVM.

> Después de actualizar el nombre de host de la base de datos de destino en el perfil, solo se cambia el nombre de host de la base de datos de destino. Se conservan todos los demás parámetros de configuración establecidos en el perfil.

Después de actualizar el nuevo nombre de host de la base de datos de destino en un perfil habilitado para la protección, se conservan el mismo conjunto de datos y las mismas políticas de protección para el perfil actualizado.

Después de cambiar el nombre de host del host objetivo, debe asegurarse de actualizar el nombre de host

para todos los perfiles protegidos existentes antes de crear los nuevos perfiles protegidos. Para actualizar el nombre de host de un perfil, ejecute el comando smo profile update.

Después de actualizar el nombre de host de la base de datos de destino, no se puede omitir o dividir el clon o desmontar el backup si el clon o el backup montado no están disponibles en el nuevo host. En tales situaciones, ejecutar las operaciones de SnapManager desde el host nuevo conlleva el fallo y las entradas obsoletas del host anterior. Para realizar operaciones de SnapManager, debe revertir al nombre de host anterior mediante la actualización de perfil.

1. Introduzca el siguiente comando: `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]`

   Las demás opciones para este comando son las siguientes:

   [-force] [-noprompt]

Si desea…	Realice lo siguiente…
Cambiar el nombre de host de la base de datos de destino	Especifique -hostnew_dB_host

2. Para ver el nombre de host de la base de datos de destino del perfil, escriba el siguiente comando: `smo profile show`

Mantener el historial de operaciones de SnapManager

SnapManager para Oracle le permite mantener el historial de operaciones de SnapManager asociadas con un único perfil o múltiples perfiles. Puede mantener el historial desde la interfaz de línea de comandos (CLI) de SnapManager o desde la interfaz gráfica de usuario (GUI). Puede ver el historial de las operaciones como un informe y utilizar el informe para fines de cumplimiento de auditoría.

Puede mantener el historial de las siguientes operaciones de SnapManager:

- Crear backup
- Verificación de backup
- Restauración de backup

- Clone create
- División de clones

La información del historial de las operaciones de SnapManager se mantiene en función de la retención. Puede configurar diferentes clases de retención para cada una de las operaciones de SnapManager admitidas.

A continuación se enumeran algunas clases de retención que puede asignar:

- Número de días
- Número de semanas
- Número de meses
- Cantidad de operaciones

Según la retención, SnapManager purga el historial automáticamente. También puede purgar manualmente el historial de las operaciones de SnapManager. Si elimina o destruye el perfil, se eliminará toda la información del historial asociada con el perfil.

> Después de revertir el host, no se pueden ver los detalles del historial ni se pueden realizar operaciones relacionadas con el historial asociadas con el perfil que se haya configurado para el mantenimiento del historial.

Configurar el historial de funcionamiento de SnapManager

SnapManager para Oracle le permite mantener el historial de operación de SnapManager desde la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager. Puede ver el historial de la operación SnapManager como un informe.

1. Para configurar el historial de la operación de SnapManager, introduzca el siguiente comando: smo history set -profile {-name, profile_name [profile_name1, profile_name2] | -all-repository [-passwwordrepo_password] -usernamerepo_username-namerepo_dbname-strepo_host -opertain_operation_weeklog | -weeklog_operation_weeklog_weeklog_1} -weekly} -weeklog_operation_weeklog_operation_weeklog_weeklog_weekly} -weeklog_operation_weeklog_weeklog_weeklog_weeklog_weekly}

```
        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
```

Ver una lista del historial de operaciones de SnapManager

Puede ver el historial de todas las operaciones de SnapManager específicas o como un

informe de acuerdo con la configuración de retención.

1. Para ver una lista de operaciones de historial de SnapManager, introduzca el siguiente comando: `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]`

Ver el historial detallado de una operación específica asociada a un perfil

Es posible ver el historial detallado de una operación SnapManager específica asociada con un perfil.

1. Para mostrar información detallada del historial de una operación de SnapManager específica asociada con un perfil, escriba el siguiente comando: `smo history operation-show -profileprofile_name {-labellabel | -idid} [-quiet | -verbose]`

Eliminando historial de operación de SnapManager

Puede eliminar el historial de la operación SnapManager si ya no se necesitan los detalles del historial.

1. Para eliminar el historial de operación de SnapManager, introduzca el siguiente comando: `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]`

Eliminar la configuración del historial asociada a un único perfil o a varios perfiles

SnapManager permite eliminar la configuración del historial de una operación SnapManager. Esta operación purga toda la información del historial asociada con un único perfil o múltiples perfiles.

1. Para eliminar el historial de las operaciones de SnapManager asociadas con un único perfil o múltiples perfiles, escriba el siguiente comando: `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]`

Ver detalles de configuración del historial de SnapManager

Puede ver la configuración del historial de un único perfil.

La operación del historial de SnapManager muestra la siguiente información para cada perfil:

- Nombre de la operación

- Clase de retención
- Recuento de retención
  a. Para mostrar la información sobre la operación del historial de SnapManager de un perfil específico, introduzca el siguiente comando: `smo history show -profileprofile_name`

Referencia de comandos de SnapManager para Oracle

La referencia del comando SnapManager incluye la sintaxis de uso, las opciones, los parámetros y los argumentos que debe proporcionar con los comandos, junto con ejemplos.

Los siguientes problemas se aplican al uso de comandos:

- Los comandos distinguen mayúsculas de minúsculas.
- SnapManager acepta hasta 200 caracteres y etiquetas de hasta 80 caracteres.
- Si el shell del host limita el número de caracteres que pueden aparecer en una línea de comandos, puede utilizar el comando cmdfile.
- No utilice espacios en nombres de perfiles ni nombres de etiquetas.
- En la especificación del clon, no utilice espacios en la ubicación del clon.

SnapManager puede mostrar tres niveles de mensajes en la consola:

- Mensajes de error
- Mensajes de advertencia
- Mensajes informativos

Puede especificar cómo desea que se muestren los mensajes. Si no especifica nada, SnapManager solo muestra mensajes de error y advertencias en la consola. Para controlar la cantidad de salida que SnapManager muestra en la consola, utilice una de las siguientes opciones de línea de comandos:

- -Quiet: Sólo muestra mensajes de error en la consola.
- -Verbose: Muestra mensajes de error, advertencia y informativos a la consola.

> Independientemente del comportamiento predeterminado o del nivel de detalle especificado para la pantalla, SnapManager siempre escribe todos los tipos de mensaje en los archivos de registro.

El comando smo_Server restart

Este comando reinicia el servidor host SnapManager y se introduce como root.

Sintaxis

```
        smo_server restart
[-quiet | -verbose]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Comando de ejemplo

En el ejemplo siguiente se reinicia el servidor host.

```
smo_server restart
```

El comando start smo_Server

Este comando inicia el servidor host que ejecuta el software SnapManager para Oracle.

Sintaxis

```
        smo_server start
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Comando de ejemplo

En el ejemplo siguiente se inicia el servidor host.

```
smo_server start
SMO-17100: SnapManager Server started on secure port 25204 with PID 11250
```

El comando de estado del servidor smo_server

Puede ejecutar el comando status de smo_Server para ver el estado del servidor host

SnapManager.

Sintaxis

```
        smo_server status
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Ejemplo

En el siguiente ejemplo, se muestra el estado del servidor de host:

```
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.
```

El comando smo_Server stop

Este comando detiene el servidor host de SnapManager y se introduce en la raíz.

Sintaxis

```
        smo_server stop
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Comando de ejemplo

En el ejemplo siguiente se utiliza el comando smo_Server stop.

```
smo_server stop
```

El comando smo backup create

El comando backup create permite crear backups de base de datos en uno o varios sistemas de almacenamiento.

Sintaxis

> Antes de ejecutar este comando, debe crear un perfil de base de datos mediante el comando profile create.

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos de la que desea realizar backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-opción automática**

Si la base de datos está en estado montado o sin conexión, SnapManager realiza un backup sin conexión. Si la base de datos está en estado abierto o en línea, SnapManager realiza un backup en línea. Si se utiliza la opción -force con la opción -offline, SnapManager fuerza un backup sin conexión aunque la base de datos esté actualmente en línea.

- **-opción en línea**

  Especifica un backup de base de datos en línea.

  Es posible crear un backup en línea de una base de datos de Real Application Clusters (RAC), siempre que el primario se encuentre en estado abierto o el primario se monte y una instancia se encuentre en estado abierto. Puede utilizar la opción -force para backups en línea si la instancia local está en estado de apagado o no hay ninguna instancia en estado abierto. La versión de Oracle debe ser 10.2.0.5; de lo contrario, la base de datos se bloqueará si existe alguna instancia en el RAC montada.

  - Si la instancia local está en estado de apagado y al menos una instancia está en estado abierto, puede utilizar la opción -force para cambiar la instancia local al estado montado.
  - Si ninguna instancia está en estado abierto, puede utilizar la opción -force para cambiar la instancia local al estado abierto.

- **-opción sin conexión**

  Especifica una copia de seguridad sin conexión mientras la base de datos está en estado de apagado. Si la base de datos está en estado abierto o montado, el backup genera errores. Si se utiliza la opción -force, SnapManager intenta modificar el estado de la base de datos para cerrar la base de datos con el fin de realizar una copia de seguridad sin conexión.

- **-opción completa**

  Realiza un backup de toda la base de datos. Esto incluye todos los datos, registros archivados y archivos de control. Se realiza una copia de seguridad de los redo logs archivados y de los archivos de control, independientemente del tipo de copia de seguridad que realice. Si se desea realizar un backup solo de una parte de la base de datos, se deben utilizar la opción -files o -tablespaces.

- **-opción de datos**

  Especifica los archivos de datos.

- **-lista de archivos**

  Realiza un backup solo de los archivos de datos especificados, además de los archivos de registro y control archivados. Separe la lista de nombres de archivo con espacios. Si la base de datos se encuentra en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-tablespaces**

  Realiza un backup solo de los espacios de tablas de la base de datos especificados, además de los archivos de registro y control archivados. Separe los nombres de tablespace con espacios. Si la base de datos se encuentra en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- * etiqueta*

  Especifica un nombre opcional para este backup. Este nombre debe ser único dentro del perfil. El nombre puede contener letras, números, guiones bajos (_) y guiones (-). No puede comenzar con un guión. Si no

se especifica una etiqueta, SnapManager crea una etiqueta predeterminada en el formato scope_type_date:

- El ámbito es F indicar un backup completo o P para indicar un backup parcial.
- El tipo es C para indicar una copia de seguridad sin conexión (en frío), H para indicar una copia de seguridad en línea (activa) o A para indicar una copia de seguridad automática, por ejemplo, P_A_20081010060037IST.
- Fecha es el año, el mes, el día y la hora de la copia de seguridad.

  SnapManager se usa un reloj de 24 horas.

Por ejemplo, si realizó un backup completo con la base de datos sin conexión el 16 de enero de 2007, a las 5:45:16 Hora estándar del este, SnapManager crearía la etiqueta F_C_20070116174516EST.

- **-cadena de comentario**

  Especifica un comentario opcional para describir esta copia de seguridad. La cadena debe escribirse entre comillas simples (').

  > Algunos vaciados despegan las comillas. En este caso, se debe incluir la comillas con una barra diagonal inversa (\). Por ejemplo, es posible que deba introducir la siguiente información: `\' this is a comment\'`.

- **-verificar opción**

  Verifica que los archivos de la copia de seguridad no están dañados ejecutando la utilidad oracle dbv.

  > Si se especifica la opción -Verify, la operación de backup no se completará hasta que finalice la operación de verificación.

- **-opción de fuerza**

  Fuerza un cambio de estado si la base de datos no está en el estado correcto. Por ejemplo, SnapManager puede cambiar el estado de la base de datos de en línea a sin conexión, según el tipo de backup especificado y el estado en el que está la base de datos.

  Con un backup de base de datos de RAC en línea, utilice la opción -force si la instancia local está en estado apagado o no hay ninguna instancia en estado abierto.

  > La versión de Oracle debe ser 10.2.0.5; de lo contrario, la base de datos se bloqueará si existe alguna instancia en el RAC montada.

  - Si la instancia local está en estado de apagado y al menos una instancia está en estado abierto, el uso de la opción -force cambia la instancia local al estado montado.
  - Si ninguna instancia está en el estado abierto, con la opción -force , la instancia local cambia al estado abierto.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

- **-protect | -noprotect | -protectadow**

  Indica si el backup debe protegerse a un almacenamiento secundario. La opción -noProtect especifica que el backup no debe protegerse en el almacenamiento secundario. Solo se protegen los backups completos. Si se especifica ninguna de las dos opciones, SnapManager protege el backup como predeterminado si el backup es un backup completo y el perfil especifica una política de protección. La opción -protectnow sólo se aplica a Data ONTAP en 7-Mode. La opción especifica que el backup se proteja inmediatamente en el almacenamiento secundario.

- **-retener { -hora | -diario | -semanal | -mensual | -ilimitado}**

  Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si no se especifica la opción -retain, la clase de retención predeterminada es la opción -Hourly. Para retener las copias de seguridad para siempre, utilice la opción -Unlimited. La opción -Unlimited hace que el backup no sea apto para que lo elimine la política de retención.

- **-archivelogs opción**

  Crea un backup de registro de archivos.

- **-backup-más extraño path1, [, [path2]]**

  Especifica los destinos de registros de archivos que se incluirán en el backup para el backup de registros de archivos.

- **-exclude-más extraño path1, [, [path2]]**

  Especifica los destinos de registro de archivos que se excluirán de la copia de seguridad.

- **-prunelogs {-all | -until-scnuntil-scn | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-meses | -días | -semanas | -horas}**

  Elimina los archivos de registro de archivos de los destinos de registro de archivos según las opciones proporcionadas al crear un backup. La opción -all elimina todos los archivos de registro de archivos de los destinos de registro de archivos. La opción -until-scn elimina los archivos de registro de archivos hasta que se especifique un número de cambio de sistema (SCN). La opción -until-date elimina los archivos de registro de archivos hasta el periodo de tiempo especificado. La opción -before elimina los archivos de registro de archivos antes del periodo de tiempo especificado (días, meses, semanas, horas).

- **-prune-dest prune_dest1,prune_dest2**

  Elimina los archivos de registro de archivos de los destinos de registro de archivos mientras se crea el backup.

- **-tasktaskspec**

  Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Se debe proporcionar la ruta completa del archivo XML al proporcionar la opción -taskspec .

- **-opción de volcado**

  Recoge los archivos de volcado después de una operación de backup de base de datos con errores o realizada correctamente.

Comando de ejemplo

El siguiente comando crea un backup completo en línea, crea un backup en el almacenamiento secundario y establece la política de retención en diaria:

```
smo backup create -profile SALES1 -full -online
-label full_backup_sales_May -profile SALESDB -force -retain -daily
Operation Id [8abc01ec0e79356d010e793581f70001] succeeded.
```

Información relacionada

Creación de backups de la base de datos

El comando smo profile create

Restaurar backups protegidos a partir del almacenamiento secundario

El comando smo backup delete

Puede ejecutar el comando backup delete para quitar backups que no se quitan automáticamente, como los backups que se usaron para crear un clon o backups que generaron errores. Puede eliminar backups retenidos de forma ilimitada sin cambiar la clase de retención.

Sintaxis

```
        smo backup delete
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la base de datos asociada con el backup que desea quitar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Especifica la copia de seguridad con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Especifica el backup con la etiqueta especificada. Opcionalmente, especifique el alcance del backup como archivo de datos o registro de archivo.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-todo**

  Especifica todos los backups. Para eliminar solo los backups especificados, use la opción -id o -label.

- **-dump**

  Recopila los archivos de volcado después de una operación de eliminación de backup realizada correctamente o con errores.

- **-fuerza**

  Fuerza la eliminación del backup. SnapManager elimina el backup incluso si hay problemas para liberar los recursos asociados con el backup. Por ejemplo, si el backup se catalogó con Oracle Recovery Manager (RMAN), pero la base de datos de RMAN ya no existe, incluido -force elimina el backup aunque no pueda conectarse con RMAN.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se elimina el backup:

```
smo backup delete -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Información relacionada

Eliminar backups

El comando smo profile create

El comando smo profile update

El comando libre de backup de smo

Puede ejecutar el comando backup free para liberar las copias Snapshot de los backups sin eliminar los metadatos de backup del repositorio.

Sintaxis

```
        smo backup free
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil asociado al backup que desea liberar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Especifica los recursos del backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup. Incluye la opción -verbose para mostrar los ID de backup.

- * etiqueta*

  Especifica el backup con la etiqueta especificada.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-todo**

  Especifica todos los backups. Para eliminar los backups especificados, use la opción -id o -label.

- **-fuerza**

  Fuerza la eliminación de las copias snapshot.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se libera el backup:

```
smo backup free -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Información relacionada

Liberando backups

El comando smo backup list

Puede ejecutar el comando backup list para ver información sobre los backups de un perfil, incluida la información sobre la clase de retención y el estado de protección.

Sintaxis

```
        smo backup list
-profile profile_name
-delimiter character
[-data | -archivelogs | -all]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea mostrar las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- * carácter delimitador*

  Muestra cada fila en una línea diferente. Los atributos de la fila están separados por el carácter especificado.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola. Incluye la opción -verbose para mostrar los ID de backup.

Ejemplo

En el ejemplo siguiente se enumeran las copias de seguridad del perfil SALES1:

```
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
```

Información relacionada

Ver una lista de backups

El comando de montaje de backup de smo

Puede ejecutar el comando backup Mount para montar un backup y realizar una operación de recuperación con una herramienta externa.

Sintaxis

```
        smo backup mount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
[-host  host]
\[-from-secondary \{-copy-id id\}\]
\[-dump\]
[-quiet | -verbose]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil asociado con el backup que desea montar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Monta la copia de seguridad con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Monta la copia de seguridad con la etiqueta especificada.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-de-secundario -copy-id**

  Monta el backup desde el almacenamiento secundario. Si no se especifica esta opción, SnapManager monta el backup desde el almacenamiento principal. Puede utilizar esta opción si se libera el backup.

  Debe especificar la opción -copy-id siempre que especifique la opción -from-secondary. Si existe más de un backup en el sistema de almacenamiento secundario, la opción -copy-id se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe utilizar para montar el backup.

  > Si se utiliza Data ONTAP en 7-Mode, es necesario especificar un valor válido para la opción -copy-id. Sin embargo, si utiliza Clustered Data ONTAP, la opción -copy-id no es necesaria.

- **-host**

  Especifica el host en el que desea montar el backup.

- **-dump**

  Recopila los archivos de volcado después de la operación de montaje correcta o con errores.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Debe utilizar este comando sólo si utiliza una herramienta externa como Oracle Recovery Manager (RMAN). SnapManager se encarga automáticamente del montaje de backups si se utiliza el comando smo backup restore para restaurar el backup. Este comando muestra una lista, que muestra las rutas donde se han montado las copias Snapshot. Esta lista solo se muestra cuando se especifica la opción -verbose.

Ejemplo

En el ejemplo siguiente se monta la copia de seguridad:

```
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.
```

Información relacionada

Montar backups

El comando smo backup restore

Se puede ejecutar el comando backup restore para restaurar backups de una base de datos o una parte de una base de datos y, opcionalmente, recuperar la información de la base de datos.

Sintaxis

```
        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 \[, path2\]\]
\[-taskspec taskspec\]
\[-dump\]
\[-force\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la base de datos que desea restaurar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre de etiqueta**

  Restaura el backup con la etiqueta especificada.

- **-id guid**

  Restaura el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- **Elija todos los archivos o especificados**

  De manera opcional, puede utilizar una de las siguientes opciones:

  - -Complete: Restaura todos los archivos de datos de la copia de seguridad.
  - -Tableslist: Restaura sólo los tablespaces especificados a partir de la copia de seguridad.

    Debe utilizar espacios para separar los nombres en la lista.

  - -Fileslist: Restaura sólo los archivos de datos especificados de la copia de seguridad.

    Debe utilizar espacios para separar los nombres en la lista. Si la base de datos se está ejecutando, SnapManager garantiza que el tablespace que contiene los archivos esté sin conexión.

- **-controlfiles**

  Restaura los archivos de control. SnapManager permite restaurar archivos de control junto con los archivos de datos de los backups en una única operación. La opción -controlfiles es independiente de otros parámetros de alcance de restauración, como -complete, -tablespaces y -files.

- **-recover**

  Recupera la base de datos después de restaurarla. También debe especificar el punto en el que desea que SnapManager recupere la base de datos mediante una de las siguientes opciones:

  - -Nologs: Recupera la base de datos al momento de la copia de seguridad y no aplica registros.

    Este parámetro se puede usar para backups en línea o sin conexión.

  - -Alllogs: Recupera la base de datos a la última transacción o confirmación y aplica todos los registros requeridos.
  - -Hasta fecha: Recupera la base de datos hasta la fecha y hora especificadas.

    Debe usar el formato year-month-date: Hour: Minute: Second (yyyy-mm-dd:hh:mm:ss). Para horas, utilice el formato de 12 o 24 horas, según la configuración de la base de datos.

  - -Until scn: Permite avanzar los archivos de datos hasta alcanzar el número de cambio de sistema (SCN) especificado.
  - -Using-backup-Controlfile: Recupera la base de datos utilizando el archivo de control de copia de seguridad.

- **-restaurespec**

  Permite restaurar los datos en un sistema de archivos activo y restaurar desde los datos especificados mediante la asignación de cada copia Snapshot original a su sistema de archivos activo. Si no especifica una opción, SnapManager restaura los datos desde las copias Snapshot en el almacenamiento principal. Es posible especificar una de las siguientes opciones:

  - -Restoreespec: Especifica los datos que se van a restaurar y el formato de restauración.
  - -Desde-secondary: Restaura los datos desde el almacenamiento secundario.

    No puede utilizar esta opción si el backup existe en el almacenamiento principal; debe liberarse el backup principal antes de poder restaurar un backup desde el almacenamiento secundario. Si se utiliza un volumen temporal, se debe especificar el volumen con la opción -temp-volume.

    Debe especificar la opción -copy-id siempre que especifique la opción -from-secondary. Si existe más de un backup en el sistema de almacenamiento secundario, la opción -copy-id se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe usar para la operación de restauración.

    > Si se utiliza Data ONTAP en 7-Mode, es necesario especificar un valor válido para la opción -copy-id. Sin embargo, si utiliza Clustered Data ONTAP, la opción -copy-id no es necesaria

    Cuando se restaura a partir de un almacenamiento secundario, SnapManager intenta en primer lugar restaurar los datos directamente desde el sistema de almacenamiento secundario al sistema de almacenamiento primario (sin afectar el host). Si SnapManager no puede realizar este tipo de restauración (por ejemplo, si los archivos no forman parte del sistema de archivos), SnapManager

recuperará una restauración de copia de archivos del lado del host. SnapManager tiene dos métodos para realizar una restauración de copia de archivos en el lado del host desde secundario. El método que selecciona SnapManager se configura en el archivo smo.config.

- Directo: SnapManager clona los datos en el almacenamiento secundario, monta los datos clonados del sistema de almacenamiento secundario en el host, y después copia los datos del clon en el entorno activo.

  Esta es la directiva de acceso secundaria predeterminada.

- Indirecto: SnapManager copia primero los datos en un volumen temporal en el sistema de almacenamiento primario, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo.

  Esta política se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Las restauraciones mediante el método indirecto demorarán el doble de tiempo que la política de acceso secundario directo, ya que se realizan dos copias de los datos.

La decisión de utilizar el método directo o indirecto se controla mediante el valor del parámetro restore.secondaryAccessPolicy del archivo de configuración smo.config.

- **-preview**

  Muestra la siguiente información:

  - Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se utilizará para restaurar cada archivo
  - Por qué no se han utilizado mecanismos más eficientes para restaurar cada archivo, al especificar la opción -verbose Si está utilizando la opción -preview , debe saber lo siguiente:
  - La opción -force no afecta al comando.
  - La opción -recover no afecta al comando.
  - La opción -fast (-require, -override, -fallback o -off) tiene un impacto significativo en la salida. Para obtener una vista previa de la operación de restauración, se debe montar la base de datos. Si desea obtener la vista previa de un plan de restauración y la base de datos no está montada actualmente, SnapManager monta la base de datos. Si no se puede montar la base de datos, el comando fallará y SnapManager devolverá la base de datos a su estado original.

  La opción -preview muestra hasta 20 archivos. Puede configurar el número máximo de archivos que se mostrará en el archivo smo.config.

- **-rápido**

  Permite elegir el proceso que se usará en la operación de restauración. Si se cumplen todas las condiciones obligatorias de restauración, es posible forzar a SnapManager para que use el proceso de restauración rápida basado en volúmenes en lugar de otros procesos de restauración. Si no se sabe que no puede realizarse una restauración de volumen, también puede usar este proceso para impedir que SnapManager realice comprobaciones de cumplimiento y la operación de restauración mediante el proceso de restauración rápido.

  La opción -fast incluye los siguientes parámetros:

  - -Require: Permite forzar a SnapManager a realizar una restauración de volúmenes, si se cumplen todas las condiciones de elegibilidad de la restauración.

Si especifica la opción -fast, pero no especifica ningún parámetro para -FAST, SnapManager utiliza el parámetro -require como valor predeterminado.

- -Override: Permite anular las comprobaciones de elegibilidad no obligatorias y realizar el proceso de restauración rápida basado en volúmenes.
- -Fallback: Permite restaurar la base de datos con el método que SnapManager determine.

  Si no se especifica la opción -FAST, SnapManager utiliza la opción default backup restore -fast fallback.

- -OFF: Le permite evitar el tiempo necesario para realizar las comprobaciones de elegibilidad.

- **-recover-from-location**

  Especifica la ubicación del registro de archivos externo de los archivos de registro de archivos. SnapManager toma los archivos de registro de archivos de la ubicación externa y los utiliza para el proceso de recuperación.

- **-taskspec**

  Especifica el archivo XML de especificación de la tarea para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de restauración. Debe proporcionar la ruta de acceso completa del archivo XML de especificación de la tarea.

- **-dump**

  Especifica recoger los archivos de volcado después de la operación de restauración.

- **-fuerza**

  Si es necesario, cambia el estado de la base de datos a uno más bajo que el estado actual. En Real Application Clusters (RAC), debe incluir la opción -force si SnapManager tiene que cambiar el estado de cualquier instancia de RAC a un estado inferior.

  De forma predeterminada, SnapManager puede cambiar el estado de la base de datos a más alto durante una operación. Esta opción no es necesaria para que SnapManager cambie el estado de la base de datos a uno más alto.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola. Puede usar esta opción para ver por qué no se pueden usar procesos de restauración más eficientes para restaurar el archivo.

Ejemplo

En el siguiente ejemplo se restaura una base de datos junto con los archivos de control:

```
smo backup restore -profile SALES1 -label full_backup_sales_May
-complete -controlfiles -force
```

Información relacionada

Restaurar backups de base de datos

Restaurar backups desde una ubicación alternativa

Creando especificaciones de restauración

El comando smo backup show

Puede usar el comando backup show para ver información detallada sobre un backup, incluido el estado de la protección, la clase de retención de backup y los backups en el almacenamiento principal y secundario.

Sintaxis

```
        smo backup show
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que se mostrarán las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- * etiqueta*

  Especifica la etiqueta del backup.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-id**

  Especifica el ID del backup.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y

advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos de la consola, al igual que cualquier información de clonación y verificación.

Ejemplo

El siguiente ejemplo muestra información detallada sobre el backup:

```
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
```

Información relacionada

Ver los detalles de backup

El comando de desmontaje del backup de smo

Puede ejecutar el comando backup umount para desmontar un backup.

Sintaxis

```
        smo backup unmount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea desmontar un backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id**

  Desmonta el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Desmonta el backup con la etiqueta especificada.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-dump**

  Recoge los archivos de volcado después de una operación de desmontaje correcta o con errores.

- **-fuerza**

  Desmonta el backup incluso si hay problemas en la liberación de los recursos asociados con el backup. SnapManager intenta desmontar el backup y borrar todos los recursos asociados. El registro muestra la operación de desmontaje correcta, pero es posible que deba limpiar los recursos de forma manual si hay errores en el registro.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

A continuación se muestra un ejemplo de una operación de desmontaje:

```
# 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.
```

Información relacionada

Desmontaje de backups

El comando de actualización de backup de smo

Puede ejecutar el comando backup update para actualizar la política de retención de backups.

Sintaxis

```
        smo backup update
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-comment comment_text\]
[-quiet | -verbose]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que se actualizarán las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Verifica el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Especifica la etiqueta de backup y el alcance del backup como archivo de datos o registro de archivos.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-comment_text**

  Introduzca texto (hasta 200 caracteres) acerca de la actualización de copia de seguridad. Puede incluir espacios.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

- **-retener {-hora | -diario | -semanal | -mensual | -ilimitado}**

  Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si no se especifica -retain, la clase de retención predeterminada es -Hourly. Para retener las copias de seguridad para siempre, utilice la opción -Unlimited. La opción -Unlimited hace que la copia de seguridad no sea elegible para su eliminación.

Ejemplo

En el ejemplo siguiente se actualiza el backup para establecer la política de retención en Unlimited:

```
smo backup update -profile SALES1 -label full_backup_sales_May
-retain -unlimited -comment save_forever_monthly_backup
```

Información relacionada

Cambiar la política de retención de backups

Retención permanente de backups

Liberar o eliminar backups exentos de la política de retención

El comando smo backup verify

Es posible ejecutar el comando backup verify para ver si el backup está en un formato válido para Oracle.

Sintaxis

```
        smo backup verify
-profile profile_name
[-label backup_name \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea verificar un backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Verifica el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- **-label label_name**

  Verifica el backup con la etiqueta especificada.

- **-dump**

  Recopila los archivos de volcado después de la operación de verificación de backup realizada correctamente o con errores.

- **-fuerza**

  Fuerza a la base de datos al estado necesario para realizar la operación de verificación.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

A continuación se muestra un ejemplo de verificación del backup:

```
smo backup verify -profile SALES1 -label full_backup_sales_May -quiet
```

```
DBVERIFY - Verification starting : FILE =
+SMO_1_1161675083835/smo/datafile/data.277.582482539 ...
```

Información relacionada

Verificación de los backups de las bases de datos

El comando smo clone create

Es posible ejecutar el comando clone create para crear el clon de una base de datos incluida en el backup. Es posible clonar un backup del almacenamiento primario o secundario.

Sintaxis

```
        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 \[, path2\]\]\[-taskspec
taskspec\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-nombre del perfil**

  Especifica la base de datos que desea clonar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-backup-id guid**

  Clona el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando list-verbose de backups de smo para mostrar el GUID de cada backup.

- **-backup-label backup_label_name**

  Especifica que se clone el backup con el nombre de etiqueta especificado.

- **-corriente**

  Especifica la creación de backup y clonado a partir del estado actual de la base de datos.

  > Si la base de datos se encuentra en el modo noarchivelog, SnapManager creará un backup sin conexión.

- **-newsid new_sid**

  Especifica un nuevo identificador exclusivo del sistema de Oracle para la base de datos clonada. El valor identificador del sistema es un máximo de ocho caracteres. Oracle no permite la ejecución simultánea de dos bases de datos con el mismo identificador de sistema en el mismo host.

- **-host target_host**

  Especifica el host en el que se debe crear el clon.

- **-label clone_label**

  Especifica una etiqueta para el clon.

- **-cadena de comentario**

  Especifica un comentario opcional para describir este clon. La cadena debe escribirse entre comillas simples.

  > Algunos vaciados eliminan las comillas. Si esto es cierto para el shell, debe escapar de las comillas con una barra invertida (\). Por ejemplo, es posible que tenga que introducir: \' esto es un comentario\'

- **-clonespec full_path_to_clonespec_file**

  Especifica la ruta de acceso al archivo XML de especificación del clon. Puede ser un nombre de ruta relativo o absoluto.

- **-asminstance**

  Especifica las credenciales que se utilizan para iniciar sesión en la instancia de ASM.

- **-asmusername asminstance_username**

  Especifica el nombre de usuario que se utiliza para iniciar sesión en la instancia de ASM.

- **-asmpassword asminstance_password**

  Especifica la contraseña que se utiliza para iniciar sesión en la instancia de ASM.

- **-syspassaword syspassaword**

  Especifica la contraseña para el usuario con privilegios sys.

  > Debe proporcionar la contraseña para el usuario con privilegios sys si las credenciales de la base de datos proporcionadas no son las mismas para el usuario con privilegios sys.

- **-reserva**

  Si se configura la opción -reserve en yes, se garantiza que la reserva de espacio garantizado para los volúmenes nuevos. Si se configura la opción -reserve en no, se garantiza que la reserva de espacio garantizado de volumen se desactive para los volúmenes clones nuevos. Si se establece la opción -reserve en heredar, se garantiza que el nuevo clon herede las características de reserva de espacio de la copia Snapshot primaria. El valor predeterminado es no

  En la siguiente tabla se describen los métodos de clonado y su efecto en la operación clone create y su opción -reserve. Una LUN se puede clonar mediante cualquiera de estos métodos.

Método de clonación	Descripción	Resultado
`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.` +

- **-desde-secundario [-copy-idcopy_id]**

  Especifica que SnapManager debe clonar una copia de un backup que se protegió en el almacenamiento

secundario. Si no se especifica esta opción, SnapManager clona la copia desde el almacenamiento principal.

Debe especificar la opción -copy-id siempre que especifique la opción -from-secondary. Si existe más de un backup en el sistema de almacenamiento secundario, la opción -copy-id se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe usar para clonar.

> Si se utiliza Data ONTAP en 7-Mode, es necesario especificar un valor válido para la opción -copy-id. Sin embargo, si utiliza Clustered Data ONTAP, la opción -copy-id no es necesaria.

- **-no-resetlogs**

  Especifica omitir la recuperación de la base de datos, ejecutar la utilidad DBNEWID y no abrir la base de datos con los registros de nuevo mientras se crea el clon.

- **-recover-from-location**

  Especifica la ubicación del registro de archivos externo de los backups de registros de archivos donde SnapManager toma los archivos de registro de archivos de la ubicación externa y los utiliza para la clonado.

- **-taskspec**

  Especifica el archivo XML de especificación de la tarea para la actividad de procesamiento previo o la actividad de procesamiento posterior de la operación de clonado. Debe proporcionar la ruta de acceso completa del archivo XML de especificación de la tarea.

- **-dump**

  Especifica recoger los archivos de volcado después de la operación de creación de clones.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se clona el backup mediante una especificación de clon que se crea para este clon:

```
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.
```

Información relacionada

Creando especificaciones de clon

Clonar bases de datos a partir de backups

El comando smo clone delete

Puede ejecutar el comando clone delete para eliminar un clon. No es posible eliminar un clon si utiliza algún operación.

Sintaxis

```
        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
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil que contiene el clon que se va a eliminar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-fuerza**

  Elimina el clon incluso si hay recursos asociados con el clon.

- **-id guid**

  Especifica el GUID del clon que se va a eliminar. SnapManager genera el GUID cuando se crea un clon. Puede usar el comando smo clone list para mostrar el GUID de cada clon.

- **-nombre de etiqueta**

  Especifica la etiqueta del clon que se va a eliminar.

- **-asminstance**

  Especifica las credenciales que se utilizan para iniciar sesión en la instancia de Automatic Storage Management (ASM).

- **-asmusername asminstance_username**

Especifica el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.

- **-asmpassword asminstance_password**

  Especifica la contraseña utilizada para iniciar sesión en la instancia de ASM.

- **-syspassaword syspassaword**

  Especifica la contraseña para el usuario con privilegios sys.

  > Debe proporcionar la contraseña para el usuario con privilegios sys si las credenciales de la base de datos proporcionadas no son las mismas para el usuario con privilegios sys.

- **-login**

  Permite introducir los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos.

- **-puerto db_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que describe el perfil.

- **-dump**

  Especifica que se recopilen los archivos de volcado después de la operación de eliminación de clones.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se elimina el clon:

```
smo clone delete -profile SALES1 -label SALES_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

El comando smo clone list

Este comando enumera los clones de la base de datos para un perfil determinado.

Sintaxis

```
        smo clone list
-profile profile_name
-delimiter character
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la lista de clones asociados con el perfil. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- * carácter delimitador*

  Cuando se especifica este parámetro, el comando enumera los atributos de cada fila separados por el carácter especificado.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se enumeran los clones de base de datos del perfil SALES1.

```
smo clone list -profile SALES1 -verbose
```

```
ID Status SID Host Label Comment
-------- ------- ----- ------- ---------- -------
8ab...01 SUCCESS hsdbc server1 back1clone test comment
```

Información relacionada

Ver una lista de clones

El comando smo clone show

Puede ejecutar el comando clone show para mostrar información sobre los clones de las bases de datos del perfil especificado.

Sintaxis

```
        smo clone show
-profile profile_name
\[-id  guid \| -label clone_name\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la lista de clones asociados con el perfil. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Muestra información sobre el clon con el GUID especificado. SnapManager genera el GUID cuando se crea un clon. Puede usar el comando smo clone show para mostrar el GUID de cada clon.

- **-label label_name**

  Muestra información sobre el clon con la etiqueta especificada.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se muestra información sobre el clon:

```
smo clone show -profile SALES1 -label full_backup_sales_May -verbose
```

En la siguiente salida se muestra información sobre un clon de un backup en el almacenamiento primario:

```
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
```

En el siguiente resultado, se muestra información sobre un clon de un backup protegido en el almacenamiento secundario:

```
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: 8abc01ec1651488301651488b580001
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
```

Información relacionada

Visualización de información detallada de los clones

El comando de plantilla de clon de smo

Este comando permite crear una plantilla de especificación de clon.

Sintaxis

```
        smo clone template
-profile name
\[-backup-id guid  \| -backup-label backup_name\]
\[-quiet \| -verbose\]
```

Parámetros

- **-nombre del perfil**

  Especifica la base de datos que desea crear una especificación de clon de. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-backup-id guid**

  Crea una especificación de clon a partir del backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Utilice el comando smo backup list para mostrar el GUID de cada backup.

- **-backup-label backup_label_name**

  Crea una especificación de clonado a partir del backup con la etiqueta de backup especificada.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo, se crea una plantilla de especificación de clon a partir del backup con la etiqueta full_backup_sales_May. Una vez completado el comando de plantilla de clon de smo, la plantilla de especificación del clon se completa.

```
smo clone template -profile SALES1 -backup-label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Información relacionada

Creando especificaciones de clon

Clonar bases de datos a partir de backups

El comando smo clone update

Este comando actualiza información acerca del clon. Puede actualizar el comentario.

Sintaxis

```
        smo clone update
-profile profile_name
\[-label label \| -id id\]
-comment  commment_text
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil que contiene el clon que desea actualizar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id**

  Especifica el ID del clon. SnapManager genera el ID cuando crea un clon. Use el comando smo clone list para mostrar el ID de cada clon.

- * etiqueta*

  Especifica la etiqueta del clon.

- **-comentario**

  Muestra el comentario introducido en la creación del clon. Este es un parámetro opcional.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se actualiza el comentario del clon.

```
smo clone update -profile anson.pcrac5
-label clone_pcrac51_20080820141624EDT -comment See updated clone
```

El comando smo clone split-delete

Este comando permite eliminar una entrada de ciclo de operaciones de división de clones de una base de datos del repositorio.

Sintaxis

```
        smo clone split-delete
-profile profile \[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil del clon.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon.

- **-etiqueta dividida-etiqueta**

  Especifica el nombre de etiqueta generado por el proceso de inicio de división de clones.

- **-id split-id**

  Especifica el ID único generado por el proceso de inicio de división de clones.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo clone split-estimation

Este comando permite ver la cantidad de división de clones del almacenamiento consumido.

Sintaxis

```
        smo clone split-estimate
-profile profile
\[-host hostname\]
\[-label clone-label | -id clone-id\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil del clon.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon.

- **-etiqueta clon-etiqueta**

  Especifica el nombre de etiqueta generado por el proceso de clonado.

- **-id clone-id**

  Especifica el ID único generado por el proceso de clonado.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando de división de clones de smo

Puede ejecutar el comando clone split para dividir un clon. El clon de división se independiza del clon original. SnapManager genera un nuevo perfil después de la operación de división de clones y se puede usar este perfil para gestionar el clon dividido.

Sintaxis

```
        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]
\[-quiet \| -verbose\]
```

Parámetros

- **-perfil clone-profile**

  Especifica el nombre del perfil a partir del cual se crea el clon.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon.

- **-etiqueta clon-etiqueta**

  Especifica el nombre de etiqueta generado por la operación de clonado.

- **-id clone-id**

  Especifica el ID único generado por la operación de clonado.

- **-split-label split-operation_label**

  Especifica el nombre de etiqueta generado por la operación de clonado.

- **-new-profile new-profile_name**

  Especifica el nuevo nombre de perfil que generará SnapManager después de una operación de división correcta.

- **-profile-password new-profile_password**

  Especifica la contraseña del perfil.

- **-repositorio**

  Especifica los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que reside la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto del protocolo de control de transmisión (TCP) que se utiliza para acceder al host en el que reside la base de datos del repositorio.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username repo_username**

Especifica el nombre de usuario necesario para acceder al host en el que reside la base de datos del repositorio.

- **-base de datos**

  Especifica los detalles de la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host**

  Especifica el nombre o la dirección IP del equipo host en el que reside la base de datos.

- **-sid db_sid**

  Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo mediante la opción -sid.

  Por ejemplo, si utiliza Real Application Clusters (RAC) de Oracle, debe especificar el identificador del sistema de la instancia de RAC en el nodo de RAC desde el cual se ejecuta SnapManager.

- **-login**

  Especifica los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-rman**

  Especifica los detalles que utiliza SnapManager para catalogar los backups con Oracle Recovery Manager (RMAN).

- **-controlfile**

  Especifica los archivos de control de la base de datos de destino como repositorio de RMAN en lugar de como catálogo.

- **-login**

  Especifica los detalles de inicio de sesión de RMAN.

- **-password rman_password**

  Especifica la contraseña que se utiliza para iniciar sesión en el catálogo de RMAN.

- **-username rman_username**

Especifica el nombre de usuario utilizado para iniciar sesión en el catálogo de RMAN.

- **-tnsname tnsname**

  Especifica el nombre de conexión tnsname (que se define en el archivo tsname.ora).

- **-osaccount**

  Especifica el nombre de la cuenta de usuario de la base de datos Oracle. SnapManager utiliza esta cuenta para realizar operaciones de Oracle como el inicio y el apagado. Generalmente, es el usuario propietario del software de Oracle en el host, por ejemplo, oracle.

- **-osgroup osgroup**

  Especifica el nombre del grupo de base de datos Oracle asociado a la cuenta de oracle.

  > Las variables -osaccount y -osgroup son necesarias para UNIX, pero no se permiten para bases de datos que se ejecutan en Windows.

- **-retener [-recuento n] [-duración m]] [-número n] [-duración m]] [-número n] [-duración m] [-número n] [-duración m]] [-mensual [-recuento n] [-duración m]]**

  Especifica la política de retención para un backup.

  Para cada clase de retención, se puede especificar el recuento de retención o la duración de la retención, o bien tanto. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). Por ejemplo, si especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-perfil-comentario perfil-comentario**

  Especifica el comentario de un perfil que describe el dominio del perfil.

- **-snapname-pattern patrón**

  Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han creado. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-protect -protection-policy policy_name**

  Especifica si el backup debe protegerse en el almacenamiento secundario.

  > Si -Protect se especifica sin -protection-policy, el conjunto de datos no tendrá una política de protección. Si se especifica -Protect y la política de protección no se establece cuando se crea el perfil, puede establecerlo más adelante mediante el comando de actualización de perfil de smo o el administrador de almacenamiento lo establece mediante la consola de Protection Manager.

- **-resumen-notificación**

Especifica los detalles para configurar la notificación de resumen por correo electrónico para varios perfiles en una base de datos de repositorio. SnapManager genera este correo electrónico.

- **-notificación**

  Especifica los detalles para configurar la notificación por correo electrónico para el nuevo perfil. SnapManager genera este correo electrónico. La notificación por correo electrónico permite al administrador de la base de datos recibir correos electrónicos sobre el estado correcto o con errores de la operación de base de datos que se realiza mediante este perfil.

- **-éxito**

  Especifica que la notificación de correo electrónico está habilitada para un perfil para cuando la operación de SnapManager se realiza correctamente.

- **-dirección de correo electrónico 1 dirección de correo electrónico 2**

  Especifica la dirección de correo electrónico del destinatario.

- **-tema-patrón**

  Especifica el asunto del correo electrónico.

- **-fallo**

  Especifica que la notificación por correo electrónico está habilitada para un perfil para cuando se produce un error en la operación de SnapManager.

- **-separate-archivvelog-backups**

  Especifica que el backup de registros de archivos está separado del backup del archivo de datos. Se trata de un parámetro opcional que puede proporcionar al crear el perfil. Después de separar los backups con esta opción, es posible crear backup solo de archivos de datos o backup de solo registros de archivos.

- **-retain-archivvelog-backups -horas | -daysdays | -weeksweeks| -months**

  Especifica que los backups de los registros de archivos se retendrán según la duración de la retención de los registros de archivo (horaria, diaria, semanal o mensual).

- **proteger [-protection-polipolypolypolypolypolycoloy_name] | -noprotect**

  Especifica que los archivos de registro de archivos están protegidos en función de la política de protección del registro de archivos.

  Especifica que los archivos de registro de archivos no están protegidos mediante la opción -noProtect.

- **-include-with-online-backups | -no-include-with-online-backups**

  Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

  Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

Especifica que los archivos de volcado no se recopilan después de la operación de creación de perfiles correcta.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada muestra mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando split-result de clon de smo

Sintaxis

Este comando permite ver el resultado del proceso de división de clones.

```
        smo clone split-result
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil del clon.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon.

- **-etiqueta dividida-etiqueta**

  Especifica el nombre de etiqueta generado por el proceso de inicio de división de clones.

- **-id split-id**

  Especifica un ID único generado por el proceso de inicio de división de clones.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando de parada por división de clones de smo

Este comando detiene el proceso de división de clones en ejecución.

Sintaxis

```
        smo clone split-stop
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil del clon.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon.

- **-etiqueta dividida-etiqueta**

  Especifica el nombre de etiqueta generado por el proceso de clonado.

- **-id split-id**

  Especifica el ID único generado por el proceso de clonado.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando de estado dividido de clon de smo

Este comando le permite conocer el progreso de la ejecución del proceso de división.

Sintaxis

```
        smo clone split-status
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil del clon.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon.

- **-etiqueta dividida-etiqueta**

  Especifica el nombre de etiqueta generado por el proceso de clonado.

- **-id split-id**

  Especifica el ID único generado por el proceso de clonado.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo clone detach

Después de dividir un volumen clonado de su volumen principal en Data ONTAP, se puede ejecutar el comando clone detach desde SnapManager para hacer saber a SnapManager que el volumen ya no es un clon.

Sintaxis

desacoplamiento del clon de smo -profile profile_name -label clone_label

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil a partir del cual se crea el clon.

- **-label clone_label**

Especifica el nombre generado por la operación de clonado.

Ejemplo

El siguiente comando desvincula el clon:

```
smo clone detach -profile SALES1 -label sales1_clone
```

El comando cmdfile de smo

Puede utilizar el comando cmdfile para ejecutar cualquier comando si el shell del host limita el número de caracteres que pueden aparecer en una línea de comandos.

Sintaxis

```
        smo cmdfile
-file file_name
\[-quiet \| -verbose\]
```

Puede incluir el comando en un archivo de texto y usar el comando cmdfile de smo para ejecutar el comando. Sólo puede agregar un comando en un archivo de texto. No debe incluir smo en la sintaxis de comandos.

> El comando cmdfile de smo reemplaza al comando pfile de smo. El archivo cmdsmo no es compatible con el comando pfile de smo.

Parámetros

- **-file file_name**

  Especifica la ruta de acceso al archivo de texto que contiene el comando que desea ejecutar.

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Ejemplo

En este ejemplo se crea un perfil incluyendo el comando profile create en command.txt ubicado en /tmp. A continuación, puede ejecutar el comando cmdfile de smo.

El archivo de texto contiene la siguiente información:

```
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
```

Ahora puede crear el perfil ejecutando el comando cmdfile de smo con el archivo command.txt:

```
smo cmdfile -file /tmp/command.txt
```

El comando smo credential clear

Este comando borra la caché de las credenciales de usuario de todos los recursos protegidos.

Sintaxis

```
        smo credential clear
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En este ejemplo se borran todas las credenciales del usuario que ejecuta el comando.

```
smo credential clear -verbose
```

```
SMO-20024 [INFO ]: Cleared credentials for user "user1".
```

Información relacionada

Borrar credenciales de usuario para todos los hosts, repositorios y perfiles

El comando smo credential delete

Este comando elimina las credenciales de usuario de un recurso protegido en particular.

Sintaxis

```
        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]
```

Parámetros

- **-host hostname**

  Especifica el nombre del servidor host en el que se ejecuta SnapManager.

  El parámetro -host incluye las siguientes opciones:

  - -Name host_name: Especifica el nombre del host para el que se eliminará la contraseña.
  - -Username user_name: Especifica el nombre de usuario en el host.
- **-repository -dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

  El parámetro -Repository incluye las siguientes opciones:

  - -Dbnamerepo_service_name: Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.
  - -Host repo_host: Especifica el nombre o la dirección IP del servidor host en el que se ejecuta la base de datos de repositorio.
  - -Login-username repo_username: Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.
  - -Port repo_Port: Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.
- **-profile -name profile_name**

  Especifica el perfil con el que está asociada la base de datos.

  El parámetro -profile incluye la siguiente opción:

- -Name profilename: Especifica el nombre del perfil para el que se eliminará la contraseña.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En este ejemplo se eliminan las credenciales del perfil.

```
smo credential delete -profile -name user1 -verbose
```

```
SMO-20022 [INFO ]: Deleted credentials and repository mapping
 for profile "user1" in user credentials for "user1".
```

En este ejemplo, se eliminan las credenciales del repositorio.

```
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".
```

En este ejemplo, se eliminan las credenciales del host.

```
smo credential delete -host -name Host2
```

```
SMO-20033 [INFO ]: Deleted host credentials for "Host2" in user
credentials for "user1".
```

Información relacionada

Eliminación de credenciales para recursos individuales

El comando smo credential list

Este comando enumera todas las credenciales de un usuario.

Sintaxis

```
        smo credential list
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

Este ejemplo muestra todas las credenciales del usuario que ejecuta el comando.

```
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
```

Información relacionada

Visualización de las credenciales de usuario

El comando smo credential set

Este comando permite establecer las credenciales para que los usuarios accedan a recursos seguros, como hosts, repositorios y perfiles de bases de datos. La contraseña del host es la contraseña del usuario en el host donde se ejecuta SnapManager. La contraseña del repositorio es la contraseña del usuario de Oracle que contiene el esquema del repositorio de SnapManager. La contraseña del perfil es una contraseña compuesta por la persona que crea el perfil. Para las opciones de host y repositorio, si no se incluye la opción -password opcional, se le pedirá que introduzca una contraseña del tipo especificado en los argumentos de comando.

Sintaxis

```
        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 \|
\[-profile
-name profile_name\]
\[-password password\] \]
\[-quiet \| -verbose\]
```

Parámetros

- **-host hostname**

  Especifica el nombre o la dirección IP del servidor host en el que se ejecuta SnapManager.

  El parámetro -host incluye las siguientes opciones:

  - -Name host_name: Especifica el nombre del host para el que se establecerá la contraseña.
  - -Username user_name: Especifica el nombre de usuario en el host.
  - -Password password: Especifica la contraseña del usuario en el host.
- **-repository -dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

  El parámetro -Repository incluye las siguientes opciones:

  - -Dbnamerepo_service_name: Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- -Host repo_host: Especifica el nombre o la dirección IP del servidor host en el que se ejecuta la base de datos de repositorio.
- -Login-username repo_username: Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.
- -Password password: Especifica la contraseña necesaria para acceder a la base de datos que almacena el repositorio.
- -Port repo_Port: Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-profile -name profile_name**

  Especifica el perfil con el que está asociada la base de datos.

  El parámetro -profile incluye la siguiente opción:

  - -Name profilename: Especifica el nombre del perfil para el que va a configurar la contraseña.
  - -Password password: Especifica la contraseña necesaria para acceder al perfil.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando para configurar las credenciales del repositorio

En el ejemplo siguiente se establecen credenciales para un repositorio.

```
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.
```

Ejemplo de comando para configurar las credenciales del host

Dado que las credenciales de host representan una credencial real del sistema operativo, deben incluir el nombre de usuario además de la contraseña.

```
smo credential set -host -name bismarck -username avida
Password for avida@bismarck : ********
Confirm password for avida@bismarck : ********
```

Información relacionada

Cómo mantiene SnapManager la seguridad

El comando smo history list

Este comando le permite ver una lista de detalles del historial de la operación SnapManager.

Sintaxis

```
        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\}
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica la operación SnapManager para la que se configura el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history list -profile -name PROFILE1 -operation -operations
backup -verbose
```

El comando Operation-show de historial de smo

Este comando le permite ver el historial de una operación de SnapManager específica asociada con un perfil.

Sintaxis

```
        smo history operation-show
-profile profile
\{-label label \| -id id\}
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- * etiqueta | -idid*

  Especifica el ID o la etiqueta de la operación de SnapManager para la que desea ver el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history operation-show -profile PROFILE1 -label backup1
-verbose
```

El comando smo history purge

Este comando le permite eliminar el historial de operaciones de SnapManager.

Sintaxis

```
        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\}
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica la operación SnapManager para la que se configura el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

El comando smo history remove

Este comando permite quitar el historial de operaciones de SnapManager asociadas con un único perfil, varios perfiles o todos los perfiles bajo un repositorio.

Sintaxis

```
        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\}
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica la operación SnapManager para la que se configura el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y

advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

El comando smo history set

Puede ejecutar el comando History Set para configurar las operaciones para las que desea ver el historial.

Sintaxis

```
        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]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. El nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Especifica los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

Especifica el nombre de la base de datos que almacena el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del host donde reside la base de datos del repositorio.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto del Protocolo de control de transmisión (TCP) que se utiliza para acceder a la base de datos del repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica las operaciones de SnapManager para las que se desea configurar el historial.

- **-retenga {-countretain_count | -dailydaily_count | -mensual-mensual_count | -weeklyweekly_count}**

  Especifica la clase de retención de las operaciones de creación de backup, verificación de backup, restauración y recuperación, y creación y división de clones. La clase de retención se establece en función del número de recuento de operaciones, el número de días, semanas o meses.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

El siguiente ejemplo muestra información sobre la operación de backup:

```
smo history set -profile -name PROFILE1 -operation -operations backup
-retain -daily 6
 -verbose
```

El comando smo history show

Este comando le permite ver información detallada del historial de un perfil en concreto.

Sintaxis

```
        smo history show
-profile profile
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history show -profile -name PROFILE1
 -verbose
```

El comando smo help

Puede ejecutar el comando help para mostrar información acerca de los comandos de la SnapManager y sus opciones. Si no proporciona un nombre de comando, se muestra una lista de comandos válidos. Si proporciona un nombre de comando, muestra la sintaxis de ese comando.

Sintaxis

```
        smo help
\[backup\|cmdfile\|clone\|credential\|help\|operation\|profile\|protection
-policy\|repository\|system\|version\|plugin\|diag\|history\|schedule\|not
ification\|storage\|get\]
\[-quiet \| -verbose\]
```

Parámetros

A continuación se muestran algunos nombres de comandos que puede utilizar con este comando:

- Backup

- clonar
- cmdfile
- credencial
- diag
- obtenga
- notificación
- ayuda
- historia
- funcionamiento
- plug-in
- perfil
- política de protección
- repositorio
- programación
- Reducida
- sistema
- versión

El comando remove-summary-notification de la notificación de smo

Este comando deshabilita la notificación de resumen de varios perfiles en una base de datos de repositorio.

Sintaxis

```
        smo notification remove-summary-notification
-repository
-dbname repo_service_name
-port repo_port
-host repo_host
-login -username repo_username
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login repo_username**

  Especifica el nombre de inicio de sesión necesario para acceder a la base de datos que almacena el repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

En el siguiente ejemplo se deshabilita la notificación de resumen de varios perfiles en una base de datos de repositorio.

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login -username oba5
```

El comando de notificación de actualización-resumen-notificación de smo

Puede ejecutar el comando notification update-summary-notification para habilitar la notificación de resumen para una base de datos de repositorio.

Sintaxis

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Especifica los detalles de la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos del repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos del repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del host en el que reside la base de datos del repositorio.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-email-dirección1,e-mail-dirección2**

  Especifica las direcciones de correo electrónico de los destinatarios.

- **-tema-patrón**

Especifica el patrón del asunto del correo electrónico.

- **-frequency { -daily --time daily_time | -time --time_time | -quannual --time mensual_time -date {1|2|3…|31 } | -semanal --time weekly_time -day {1|2|3|4|5|6|7 }**

  Especifica el tipo de programación y la hora de la programación en el momento en que desea recibir la notificación por correo electrónico.

- **-profile1, profile2**

  Especifica los nombres de perfil que requieren notificación por correo electrónico.

- **-notification-host-notification-host**

  Especifica el host del servidor SnapManager desde el cual se envía el correo electrónico de notificación de resumen a los destinatarios. Puede proporcionar un nombre de host o una dirección IP para el host de notificación. También es posible actualizar la dirección IP del host o el nombre de host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se habilita la notificación de resumen para una base de datos de repositorio:

```
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
```

El comando smo notification set

Puede utilizar el comando Notification Set para configurar el servidor de correo.

Sintaxis

```
        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]
```

Parámetros

- **-sender-email email_address**

  Especifica la dirección de correo electrónico del remitente desde la cual se envían las alertas por correo electrónico. En SnapManager 3.2 para Oracle, puede incluir un guión (-) al especificar el nombre de dominio de la dirección de correo electrónico. Por ejemplo, puede especificar la dirección de correo electrónico del remitente como -sender-email07lbfmdatacenter@continental-corporation.com.

- **-mailhost**

  Especifica el nombre o la dirección IP del servidor host que gestiona las notificaciones por correo electrónico.

- **-mailport**

  Especifica el número de puerto del servidor de correo.

- **-authentication -username -password**

  Especifica los detalles de autenticación de la dirección de correo electrónico. Debe especificar el nombre de usuario y la contraseña.

- **-repositorio**

  Especifica los detalles de la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto del Protocolo de control de transmisión (TCP) que se utiliza para acceder a la base de datos del repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos del repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del host donde reside la base de datos del repositorio.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo, se configura el servidor de correo:

```
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
```

El comando de volcado de la operación de smo

Puede ejecutar el comando operation dump para crear un archivo JAR que contenga información de diagnóstico acerca de una operación.

Sintaxis

```
        smo operation dump
-profile profile_name
\[-label label_name \| -id guid\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea crear los archivos de volcado. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-label label_name**

  Crea archivos de volcado para la operación y asigna la etiqueta especificada.

- **-id guid**

  Crea archivos de volcado para la operación con el GUID especificado. SnapManager genera el GUID cuando se inicia la operación.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se crea el archivo de volcado para la copia de seguridad:

```
smo operation dump -profile SALES1
-id 8abc01ec0e78f3e2010e78f3fdd00001
```

```
Dump file created
Path:/userhomedirectory/.netapp/smo/3.3/smo_dump_8abc01ec0e78f3e2010e78f3f
dd00001.jar
```

Información relacionada

Volcar archivos

El comando smo operation list

Este comando muestra la información resumida de todas las operaciones registradas en un perfil especificado.

Sintaxis

```
        smo operation list
-profile profile_name
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- * carácter delimitador*

  (Opcional) cuando se especifica este parámetro, el comando enumera cada fila en una línea independiente y los atributos de esa fila están separados por el carácter especificado.

- **-silencio**

  (Opcional) sólo muestra mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  (Opcional) muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo, se muestra la información de resumen de todas las operaciones registradas con el perfil especificado.

```
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
```

Información relacionada

Ver una lista de operaciones

El comando smo operation show

Puede ejecutar el comando operation show para mostrar la información de resumen de todas las operaciones realizadas en el perfil especificado. La salida muestra el usuario cliente (el usuario del PC cliente) y el usuario efectivo (el usuario de SnapManager que es válido en el host seleccionado).

Sintaxis

```
        smo operation show
-profile profile_name
\[-label label \| -id id\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- * etiqueta*

  Especifica la etiqueta de la operación.

- **-id**

  Especifica el identificador de la operación.

- **-silencio**

  Opcional: Muestra solo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Opcional: Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

La siguiente línea de comandos muestra información detallada sobre una operación:

```
# 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
```

Información relacionada

Ver los detalles de la operación

El comando smo password reset

Puede ejecutar el comando de restablecimiento de contraseña para restablecer la contraseña de un perfil.

Sintaxis

```
        smo password reset
-profile profile
\[-profile-password profile_password\]
\[-repository-hostadmin-password repository_hostadmin_password\]
[-quiet | -verbose]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil para el que desea restablecer la contraseña.

- **-profile-password profile_password**

  Especifica la nueva contraseña para el perfil.

- **-repository-hostadmin-password admin_password**

  Especifica la credencial de usuario autorizado con privilegios raíz para la base de datos del repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo plugin check

SnapManager le permite instalar y utilizar scripts personalizados para diversas operaciones. SnapManager ofrece plugins de backup, restauración y clonado para automatizar scripts personalizados antes y después de las operaciones de backup, restauración y clonado. Antes de utilizar el plugin de backup, restauración y clonado, puede ejecutar el comando plugin check para comprobar la instalación de los scripts de los plugins. Los scripts personalizados se almacenan en tres directorios: Política (para scripts que siempre deben ejecutarse antes de que se realice el backup, la restauración o la operación de clonado), el previo (para scripts de procesamiento previo) y el posterior (para scripts de procesamiento posterior).

Sintaxis

```
        smo plugin check

-osaccount os_db_user_name
```

Parámetro

- **-osaccount**

  Especifica el nombre de usuario de la base de datos del sistema operativo (SO). Si no se introduce la opción -osaccount, SnapManager comprueba los scripts del plugin como usuario raíz en lugar de como usuario específico.

Ejemplo

El ejemplo siguiente muestra que el comando plugin check encontró el script personalizado de la directiva 1 almacenado en el directorio de directivas como ejecutable. El ejemplo también muestra que los otros dos scripts personalizados almacenados en el directorio previo no devuelven mensajes de error (mostrados con un estado de 0); sin embargo, el cuarto script personalizado (post-plug-in1), que se encuentra en el directorio post, contiene errores (mostrados con un estado de 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.
```

Información relacionada

Clonar bases de datos y usar scripts de plugins personalizados

El comando smo profile create

Puede ejecutar el comando profile create para crear un perfil de una base de datos en un repositorio. Debe montar la base de datos antes de ejecutar este comando.

Sintaxis

```
        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]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-profile-password profile_password**

  Especifique la contraseña del perfil.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-sid db_sid**

  Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo con la opción -sid.

  Por ejemplo, si utiliza Real Application Clusters (RAC) de Oracle, debe especificar el identificador del sistema de la instancia de RAC en el nodo de RAC desde el cual se ejecuta SnapManager.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos del repositorio.

- **-base de datos**

  Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host db_host**

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-asminstance**

  Especifica las credenciales que se utilizan para iniciar sesión en la instancia de Automatic Storage Management (ASM).

- **-asmusername asminstance_username**

  Especifica el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.

- **-asmpassword asminstance_password**

  Especifica la contraseña utilizada para iniciar sesión en la instancia de ASM.

- **-login**

  Especifica los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-puerto db_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que describe el perfil.

- **-rman**

  Especifica los detalles que utiliza SnapManager para catalogar los backups con Oracle Recovery Manager (RMAN).

- **-controlfile**

  Especifica los archivos de control de la base de datos de destino en lugar de un catálogo como repositorio de RMAN.

- **-login**

  Especifica los detalles de inicio de sesión de RMAN.

- **-password rman_password**

  Especifica la contraseña que se utiliza para iniciar sesión en el catálogo de RMAN.

- **-username rman_username**

  Especifica el nombre de usuario utilizado para iniciar sesión en el catálogo de RMAN.

- **-tnsname tnsname**

  Especifica el nombre de conexión tnsname (que se define en el archivo tsname.ora).

- **-osaccount**

  Especifica el nombre de la cuenta de usuario de la base de datos Oracle. SnapManager utiliza esta cuenta para realizar operaciones de Oracle como el inicio y el apagado. Generalmente, es el usuario propietario del software de Oracle en el host, por ejemplo, oracle.

- **-osgroup osgroup**

  Especifica el nombre del grupo de base de datos Oracle asociado a la cuenta de oracle.

- **-retener [-recuento n] [-duración m]] [-número n] [-duración m]] [-número n] [-duración m] [-número n] [-duración m]] [-mensual [-recuento n] [-duración m]]**

  Especifica la política de retención para un backup donde se cuenta un número de retención o ambos, junto con una duración de retención para una clase de retención (por hora, día, semana, mes).

  Para cada clase de retención, se puede especificar un recuento de retención o una duración de retención. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). Por ejemplo, si el usuario especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-comentario**

  Especifica el comentario de un perfil que describe el dominio del perfil.

- **-snapname-pattern patrón**

  Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han creado. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-protect -política de protección**

  Indica si el backup debe protegerse a un almacenamiento secundario.

  > Si -protectis se especifica sin política de protección, el conjunto de datos no tendrá una política de protección. Si se especifica -Protect y -protection-policy no se establece cuando se crea el perfil, se puede establecer más tarde un comando bysmo profile update o bien establecer el administrador de almacenamiento a través de la consola de Protection Manager.

- **-resumen-notificación**

  Especifica que la notificación de resumen por correo electrónico está activada para el nuevo perfil.

- **-notification -success-email-mail_dirección1,dirección de correo electrónico.2 -subject_pattern**

  Especifica que la notificación de correo electrónico está habilitada para el nuevo perfil de forma que los destinatarios reciban correos electrónicos cuando la operación de SnapManager se realice correctamente. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del nuevo perfil.

También se puede incluir texto de asunto personalizado para el nuevo perfil. Puede cambiar el texto del asunto cuando cree un perfil o después de que se haya creado el perfil. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-notification -failure -email correo-e_dirección1,dirección de correo-e-dirección2 -subject_pattern**

  Especifica que la habilitación de la notificación por correo electrónico está habilitada para el nuevo perfil, de modo que los destinatarios reciban los correos electrónicos cuando falle la operación de SnapManager. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del nuevo perfil.

  También se puede incluir texto de asunto personalizado para el nuevo perfil. Puede cambiar el texto del asunto cuando cree un perfil o después de que se haya creado el perfil. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-separate-archivvelog-backups**

  Especifica que el backup de registros de archivos está separado del backup del archivo de datos. Este es un parámetro opcional que puede proporcionar al crear el perfil. Después de separar el backup con esta opción, es posible tomar el backup solo de los archivos de datos o el backup de solo los registros de archivos.

- **-retain-archivvelog-backups -horas | -daysdays | -weeksweeks| -months**

  Especifica que los backups de los registros de archivos se retendrán según la duración de la retención del registro de archivos (hora, día, semana, mensual).

- **proteger [-protection-polipolypolypolypolypolycoloy_name] | -noprotect**

  Especifica la protección de los archivos de registro de archivos en función de la política de protección del registro de archivos.

  La opción -noProtect especifica no proteger los archivos de registro de archivos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

- **-include-with-online-backups**

  Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

- **-no-include-with-online-backups**

  Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

  Especifica que los archivos de volcado se recopilan después de la operación de creación de perfiles correcta.

Ejemplo

El siguiente ejemplo muestra la creación de un perfil con una política de retención de horas y notificaciones por correo electrónico:

```
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.
```

Información relacionada

Gestionar perfiles para backups eficientes

El comando smo protection-policy

Nomenclatura de copias Snapshot

Cómo SnapManager retiene los backups en el almacenamiento local

El comando smo profile delete

Puede ejecutar el comando profile delete para eliminar un perfil de la base de datos.

Sintaxis

```
        smo profile delete
-profile profile
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el perfil que se va a eliminar.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se elimina el perfil:

```
smo profile delete -profile SALES1
Operation Id [Ncaf00af0242b3e8dba5c68a57a5ae932] succeeded.
```

Información relacionada

Eliminar perfiles

El comando smo profile destroy

Este comando elimina la división de clones (base de datos) junto con el perfil que genera SnapManager durante el proceso de división de clones.

Sintaxis

```
        smo profile destroy
-profile profile
\[-host hostname\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el perfil que genera SnapManager después de un proceso de división de clones correcto.

- **-host hostname**

  Especifica el nombre de host en el que existe el clon dividido.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se elimina el perfil denominado SALES1.

```
smo profile destroy -profile SALES1
```

El comando smo profile dump

Puede ejecutar el comando profile dump para crear el archivo .jar que contiene información de diagnóstico acerca de un perfil.

Sintaxis

```
        smo profile dump
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea crear los archivos de volcado. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se crea un volcado para el perfil SALES1:

```
smo profile dump -profile SALES1
Dump file created
Path:/userhomedirectory/.netapp/smo/3.3.0/smo_dump_SALES1_hostname.jar
```

El comando smo profile list

Este comando muestra una lista de los perfiles actuales.

Sintaxis

```
        smo profile list
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se muestran los perfiles existentes con sus detalles.

```
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: ********
```

El comando smo profile show

Puede ejecutar el comando profile show para mostrar la información de un perfil.

Sintaxis

```
        smo profile show
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se muestran los detalles del perfil:

```
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)
```

El comando smo profile SYNC

Este comando carga las asignaciones de perfil a repositorio para ese repositorio en un archivo del directorio inicial en el host local.

Sintaxis

```
        smo profile sync
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login
-username repo_username
                \[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica la base de datos del repositorio para el perfil que se va a sincronizar.

- **-host**

  Especifica el host de la base de datos.

- **-puerto**

  Especifica el puerto para el host.

- **-login**

  Especifica el proceso de inicio de sesión para el usuario host.

- **-nombre de usuario**

  Especifica el nombre de usuario para el host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se muestra el resultado del comando para sincronizar las asignaciones de perfil a repositorio de la base de datos.

```
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.
```

El comando smo profile update

Puede ejecutar el comando profile update para actualizar la información de un perfil existente.

Sintaxis

```
        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]
\[-quiet \| -verbose\]
```

Parámetros

Si se ha establecido una política de protección en el perfil, no podrá cambiar la política con SnapManager. Debe cambiar la política con la consola de Protection Manager.

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-profile-password profile_password**

  Especifica la contraseña del perfil.

- **-new-profile new_profile_name**

  Especifica el nuevo nombre que puede proporcionar para un perfil.

- **-base de datos**

  Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos de la que se realizará un backup, se restaurará, etc.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-sid db_sid**

  Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo mediante la opción -sid.

  Por ejemplo, si utiliza Real Application Clusters (RAC) de Oracle, debe especificar el identificador de sistema SID de la instancia de RAC en el nodo RAC desde el cual se ejecuta SnapManager.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP necesario para acceder a la base de datos del repositorio.

- **-base de datos**

  Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos que se realizará

un backup, se restaurará o se clonará.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-login**

  Especifica los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-puerto db_port**

  Especifica el número de puerto TCP necesario para acceder a la base de datos que describe el perfil.

- **-asminstance**

  Especifica las credenciales que se utilizan para iniciar sesión en la instancia de Automatic Storage Management (ASM).

- **-asmusername asminstance_username**

  Especifica el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.

- **-asmpassword asminstance_password**

  Especifica la contraseña utilizada para iniciar sesión en la instancia de ASM.

- **-rman**

  Especifica los detalles que utiliza SnapManager para catalogar los backups con Oracle Recovery Manager (RMAN).

- **-controlfile**

  Especifica los archivos de control de la base de datos de destino en lugar de un catálogo como repositorio de RMAN.

- **-login**

  Especifica los detalles de inicio de sesión de RMAN.

- **-password rman_password**

Especifica la contraseña que se utiliza para iniciar sesión en el catálogo de RMAN.

- **-username rman_username**

  Especifica el nombre de usuario utilizado para iniciar sesión en el catálogo de RMAN.

- **-tnsname tnsname**

  Especifica el nombre de conexión tnsname (que se define en el archivo tsname.ora).

- **-remove-rman**

  Especifica la eliminación de RMAN en el perfil.

- **-osaccount**

  Especifica el nombre de la cuenta de usuario de la base de datos Oracle. SnapManager utiliza esta cuenta para realizar operaciones de Oracle como el inicio y el apagado. Generalmente, es el usuario propietario del software de Oracle en el host, por ejemplo, oracle.

- **-osgroup osgroup**

  Especifica el nombre del grupo de base de datos Oracle asociado a la cuenta de oracle.

- **-retener [-contador hora [-compensn] [-duración m]] [-diario [-conteo n] [-duración m] [-semanal [-conteo n][-duración m]] [-mensual [-conteo n][-duración m]]**

  Especifica la clase de retención (por hora, por día, por semana o por mes) para una copia de seguridad.

  Para cada clase de retención, se puede especificar un recuento de retención, una duración de retención o ambas. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora o días por día). Por ejemplo, si el usuario especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-comentario**

  Especifica el comentario de un perfil.

- **-snapname-pattern patrón**

  Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han producido. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-protect [-protection-polipolypolypolypolycoloy_name] | [-noprotect]**

  Indica si el backup debe protegerse a un almacenamiento secundario o no.

> Si -Protect se especifica sin -protection-policy, el conjunto de datos no tendrá una política de protección. Si se especifica -Protect y -protection-policy no se establece cuando se crea el perfil, puede ser establecido más tarde comando bysmo profile update o establecido por el administrador de almacenamiento mediante la consola de Protection Manager .

La opción -noProtect especifica no proteger el perfil para el almacenamiento secundario.

- **-resumen-notificación**

  Especifica que la notificación de resumen por correo electrónico está activada para el perfil existente.

- **-notificación [-success-email e-mail_dirección1,dirección de e-mail.2 -subject_pattern]**

  Habilita la notificación de correo electrónico para el perfil existente de forma que los destinatarios reciban los correos electrónicos cuando la operación SnapManager se realice correctamente. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del correo electrónico para el perfil existente.

  Puede cambiar el texto del asunto al actualizar el perfil o incluir texto de asunto personalizado. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-notificación [-failure -email e-mail_dirección1,dirección de e-mail.2 -subject_pattern]**

  Habilita la notificación de correo electrónico para el perfil existente de modo que los destinatarios reciban los correos electrónicos cuando falle la operación de SnapManager. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del correo electrónico para el perfil existente.

  Puede cambiar el texto del asunto al actualizar el perfil o incluir texto de asunto personalizado. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-separate-archivvelog-backups**

  Separa el backup de registros de archivos del backup de archivo de datos. Este es un parámetro opcional que puede proporcionar al crear el perfil. Después de separar los backups se separan con esta opción, es posible crear un backup de solo los archivos de datos o un backup de solo los registros de archivos.

- **-retain-archivvelog-backups -horas | -daysdays | -weeksweeks| -months**

  Especifica que los backups de los registros de archivos se retendrán según la duración de la retención del registro de archivos (hora, día, semana, mensual).

- **-protect [-protection-polipolypolypolypolycoloy_name] | -noprotect**

  Especifica que los archivos de registro de archivos están protegidos en función de la política de protección del registro de archivos.

  Especifica que los archivos de registro de archivos no están protegidos mediante la opción -noProtect.

- **-include-with-online-backups | -no-include-with-online-backups**

  Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

  Especifica que los archivos de volcado se recopilan después de la operación de creación de perfiles correcta.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se cambia la información de inicio de sesión de la base de datos descrita por el perfil y se configura la notificación por correo electrónico para este perfil:

```
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.
```

Información relacionada

Cambio de contraseñas de perfil

Cómo SnapManager retiene los backups en el almacenamiento local

El comando smo profile verify

Puede ejecutar el comando profile verify para verificar la configuración del perfil. Debe montar la base de datos antes de ejecutar este comando.

Sintaxis

```
        smo profile verify
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-perfil**

Especifica el perfil que se va a verificar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se verifica el perfil:

```
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.
```

Información relacionada

Verificando perfiles

El comando smo protection-policy

Puede ejecutar el comando de directiva de protección para enumerar las directivas de protección que se pueden aplicar a un perfil. La directiva de protección se puede aplicar cuando se crea un perfil nuevo o se actualiza un perfil existente. También puede establecer la política de protección del perfil mediante la consola de Protection Manager.

Sintaxis

```
smo protection-policy list
```

> Protection Manager y SnapDrive se deben instalar en el servidor para que pueda utilizar este comando.

Parámetros

- **lista**

  Muestra la lista de directivas de protección que se pueden establecer en un perfil.

Ejemplo

En el siguiente ejemplo, se enumeran las políticas de protección que se pueden configurar en un perfil:

```
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
```

Información relacionada

Gestionar perfiles para backups eficientes

El comando smo repository create

Sintaxis

Este comando crea un repositorio en el que se almacenan perfiles de base de datos y credenciales asociadas. Este comando también comprueba si el tamaño de los bloques es adecuado.

```
        smo repository create
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Se intenta forzar la creación del repositorio. Con esta opción, SnapManager se solicita que se realice un backup del repositorio antes de crear el repositorio.

- **-noprompt**

  No muestra el símbolo del sistema de realizar una copia de seguridad del repositorio antes de crearlo si utiliza la opción -force. El uso de la opción -noprompt garantiza que el prompt no aparezca, facilitando la creación de repositorios con un script.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando

El siguiente ejemplo crea un repositorio en la base de datos SMOREPO en el hotspur del host.

```
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
```

El comando smo repository delete

Este comando elimina un repositorio utilizado para almacenar perfiles de base de datos y credenciales asociadas. Sólo puede eliminar un repositorio si no hay perfiles en el repositorio.

Sintaxis

```
        smo repository delete
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-port repo_port**

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Se intenta forzar la eliminación del repositorio, incluso si hay operaciones incompletas. SnapManager emite un aviso si existen operaciones incompletas, en las que se pregunta si está seguro de que se desea eliminar el repositorio.

- **-noprompt**

  No se le solicita antes de eliminar el repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la eliminación de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando

En el ejemplo siguiente se elimina el repositorio de la base de datos SALESDB.

```
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".
```

El comando rollback del almacén de smo

Este comando permite revertir o revertir una versión superior de SnapManager a la versión original desde la que se actualizó.

Sintaxis

```
        smo repository rollback
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-rollbackhost host_with_target_database
[-force]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-rollbackhost host host_with_target_database**

  Especifica el nombre del host que se va a revertir de una versión superior de SnapManager a la versión anterior original.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

  No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smo repository rollback -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -rollbackhost hostA
```

El comando para actualizar el almacén de smo

Este comando realiza la actualización en un solo host o de varios hosts y las bases de datos de destino asociadas desde una versión inferior de SnapManager a una versión

posterior. El host actualizado solo se gestiona con la versión superior de SnapManager.

Sintaxis

```
        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]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-actualizehost host_with_target_database**

  Especifica el nombre del host que se actualizará de una versión inferior de SnapManager a una versión superior.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

  No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smo repository rollingupgrade -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -upgradehost hostA
```

El comando smo repository show

Este comando muestra información sobre el repositorio.

Sintaxis

```
        smo repository show
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del

repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando

En el siguiente ejemplo se muestran detalles sobre el repositorio de la base de datos SALESDB.

```
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
```

El comando de actualización del almacén de smo

Este comando actualiza el repositorio que almacena perfiles de base de datos y las credenciales asociadas al actualizar SnapManager. Cada vez que instale una nueva versión de SnapManager, debe ejecutar el comando de actualización del repositorio para

poder utilizar la nueva versión. Puede utilizar este comando solo si no hay comandos incompletos en el repositorio.

Sintaxis

```
        smo repository update
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

  No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521
```

El comando smo schedule create

Es posible utilizar el comando schedule create para programar la creación de un backup en un momento específico.

Sintaxis

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos para la que desea programar el backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-opción automática**

  Si la base de datos está en estado montado o sin conexión, SnapManager realiza un backup sin conexión. Si la base de datos está en estado abierto o en línea, SnapManager realiza un backup en línea. Si se utiliza la opción -force con la opción -offline, SnapManager fuerza un backup sin conexión aunque la base de datos esté actualmente en línea.

- **-opción en línea**

  Especifica un backup de base de datos en línea.

  Es posible crear un backup en línea de una base de datos de Real Application Clusters (RAC), siempre

que el primario se encuentre en estado abierto o montado y una instancia esté en estado abierto. Puede utilizar la opción -force para backups en línea si la instancia local está en el estado de apagado o no hay ninguna instancia abierta.

  - Si la instancia local está en estado de apagado y al menos una instancia está abierta, puede utilizar la opción -force para cambiar la instancia local a montada.
  - Si ninguna instancia está en estado abierto, puede utilizar la opción -force para cambiar la instancia local a abierta.

- **-opción sin conexión**

  Especifica un backup sin conexión mientras la base de datos está en estado de apagado. Si la base de datos está en estado abierto o montado, el backup genera errores. Si se utiliza la opción -force, SnapManager intenta modificar el estado de la base de datos para cerrar la base de datos con el fin de realizar una copia de seguridad sin conexión.

- **-opción completa**

  Realiza un backup de toda la base de datos. Esto incluye todos los datos, registros archivados y archivos de control. Se realiza una copia de seguridad de los redo logs archivados y de los archivos de control, independientemente del tipo de copia de seguridad que realice. Si se desea realizar un backup solo de una parte de la base de datos, se deben utilizar la opción -files o -tablespaces.

- **-lista de archivos**

  Realiza un backup solo de los archivos de datos especificados, además de los archivos de registro y control archivados. Separe la lista de nombres de archivo con espacios. Si la base de datos está en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-tablespaces**

  Realiza un backup solo de los espacios de tablas de la base de datos especificados, además de los archivos de registro y control archivados. Separe los nombres de tablespace con espacios. Si la base de datos está en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-nombre de etiqueta**

  Especifica un nombre opcional para este backup. Este nombre debe ser único dentro del perfil. El nombre puede contener letras, números, guiones bajos (_) y guiones (-). No puede comenzar con un guión.

  Si no se especifica una etiqueta, SnapManager crea una etiqueta predeterminada en el formato scope_type_date:

  - El ámbito es F indicar un backup completo o P para indicar un backup parcial.
  - El tipo es C para indicar una copia de seguridad sin conexión (en frío), H para indicar una copia de seguridad en línea (activa) o A para indicar una copia de seguridad automática, por ejemplo, P_A_20081010060037IST.
  - Fecha es el año, el mes, el día y la hora de la copia de seguridad.

    SnapManager se usa un reloj de 24 horas.

  Por ejemplo, si realizó un backup completo con la base de datos sin conexión el 16 de enero de 2007, a las 5:45:16 Hora estándar del este, SnapManager crearía la etiqueta F_C_20070116174516EST.

- **-cadena de comentario**

  Especifica un comentario opcional para describir esta copia de seguridad. La cadena debe escribirse entre comillas simples (').

  > Algunos vaciados pelan entre comillas. Si esto es cierto para el shell, debe incluir la comillas con una barra diagonal inversa (\). Por ejemplo, es posible que deba introducir: `\' this is a comment\'`.

- **-verificar opción**

  Verifica que los archivos de la copia de seguridad no están dañados ejecutando la utilidad oracle dbv.

  > Si se especifica la opción -Verify, la operación de backup no se completará hasta que finalice la operación de verificación.

- **-opción de fuerza**

  Fuerza un cambio de estado si la base de datos no está en el estado correcto. Por ejemplo, SnapManager puede cambiar el estado de la base de datos de en línea a sin conexión, según el tipo de backup especificado y el estado en el que está la base de datos.

  Con un backup de base de datos de RAC en línea, utilice la opción -force si la instancia local está en estado apagado o no hay ninguna instancia abierta.

  > La versión de Oracle debe ser 10.2.0.5; de lo contrario, la base de datos se bloqueará si existe alguna instancia en el RAC montada.

  - Si la instancia local está en estado de apagado y al menos una instancia está abierta, puede cambiar la instancia local a montada mediante la opción -force .
  - Si no hay ninguna instancia abierta, puede cambiar la instancia local a abierta mediante la opción -force.

- **-protect | -noprotect | -protectadow**

  Indica si el backup debe protegerse a un almacenamiento secundario. La opción -noProtect especifica que el backup no debe protegerse en el almacenamiento secundario. Solo se protegen los backups completos. Si se especifica ninguna de las dos opciones, SnapManager protege el backup como predeterminado si el backup es un backup completo y el perfil especifica una política de protección. La opción -protectnow sólo se aplica a Data ONTAP en 7-Mode. La opción especifica que el backup se proteja inmediatamente en el almacenamiento secundario.

- **-retener { -hora | -diario | -semanal | -mensual | -ilimitado}**

  Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si no se especifica la opción -retain, la clase de retención predeterminada es -Hourly. Para retener las copias de seguridad para siempre, utilice la opción -Unlimited. La opción -Unlimited hace que el backup no sea apto para que lo elimine la política de retención.

- **-archivelogs**

  Especifica la creación de un backup de registro de archivos.

- **-backup-más extraño path1, [, [path2]]**

  Especifica los destinos de registros de archivos para el backup de registros de archivos.

- **-exclude-más extraño path1, [, [path2]]**

  Especifica los destinos de registro de archivos que se excluirán de la copia de seguridad.

- **-prunelogs {-all | -until-scnuntil-scn | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-meses | -días | -semanas | -horas}**

  Especifica si se eliminarán los archivos de registro de archivos de los destinos de registro de archivos en función de las opciones proporcionadas al crear un backup. La opción -all elimina todos los archivos de registro de archivos de los destinos de registro de archivos. La opción -until-scn elimina los archivos de registro de archivos hasta que se especifique un número de cambio de sistema (SCN). La opción -until -date elimina los archivos de registro de archivos hasta el periodo de tiempo especificado. La opción -before elimina los archivos de registro de archivos antes del periodo de tiempo especificado (días, meses, semanas, horas).

- **-nombre-horario nombre_horario**

  Especifica el nombre que se proporcionará para la programación.

- **-schedule-comentario schedule_comment**

  Especifica un comentario opcional que se va a describir acerca de la programación del backup.

- **-interval { -time | -daily | -semanal | -mensual | -onetimeonly}**

  Especifica el intervalo de tiempo mediante el cual se crean los backups. Se puede programar el backup cada hora, día, semana, mes o solo una vez.

- **-cronstring cron_string**

  Especifica la programación del backup mediante cronstring. Las expresiones cron se utilizan para configurar instancias de CronTrigger. Las expresiones cron son cadenas que se componen de las siguientes subexpresiones:

  - 1 se refiere a segundos.
  - 2 se refiere a minutos.
  - 3 se refiere a horas.
  - 4 se refiere a un día en un mes.
  - 5 se refiere al mes.
  - 6 se refiere a un día en una semana.
  - 7 se refiere al año (opcional).

- **-hora de inicio aaaa-MM-dd HH:mm**

  Especifica la hora de inicio de la operación programada. La hora de inicio de la programación debe incluirse en el formato aaaa-MM-dd HH:mm.

- **-runasuser runasuser**

Especifica si se cambia el usuario (usuario raíz o usuario de Oracle) de la operación de backup programada mientras se programa el backup.

- **-tasktaskspec**

  Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. La ruta completa del archivo XML debe proporcionarse con la opción -taskspec .

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo schedule delete

Este comando elimina una programación de backup cuando ya no es necesaria.

Sintaxis

```
        smo schedule delete
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea eliminar una programación de backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre de programación que se proporcionó al crear una programación de backups.

El comando smo schedule list

Este comando, enumera las operaciones programadas asociadas con un perfil.

Sintaxis

```
        smo schedule list
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos, mediante el cual puede ver una lista de operaciones programadas. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

El comando smo schedule resume

Este comando reanuda la programación de backup suspendida.

Sintaxis

```
        smo schedule resume
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea reanudar la programación de backups suspendida. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre de programación que se proporcionó al crear una programación de backups.

El comando smo schedule suspend

Este comando suspende una programación de backup hasta que se reanuda la programación de backup.

Sintaxis

```
        smo schedule suspend
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea suspender una programación de backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre de programación que se proporcionó al crear una programación de backups.

El comando smo schedule update

Este comando actualiza la programación de una copia de seguridad.

Sintaxis

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea programar el backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre que se proporcionará para la programación.

- **-schedule-comentario schedule_comment**

  Especifica un comentario opcional que se va a describir acerca de la programación del backup.

- **-interval { -time | -daily | -semanal | -mensual | -onetimeonly}**

  Indica el intervalo de tiempo mediante el cual se crean los backups. Se puede programar el backup cada hora, día, semana, mes o una sola vez.

- **-cronstring cron_string**

  Especifica la programación del backup mediante cronstring. Las expresiones cron se utilizan para configurar instancias de CronTrigger. Las expresiones cron son cadenas que se componen de siete subexpresiones:

  - 1 se refiere a segundos
  - 2 se refiere a minutos
  - 3 se refiere a horas
  - 4 se refiere a un día en un mes
  - 5 se refiere al mes
  - 6 se refiere a un día en una semana
  - 7 se refiere al año (opcional)

- **-hora de inicio aaaa-MM-dd HH:mm**

  Especifica la hora de inicio de la operación de programación. La hora de inicio de la programación debe incluirse en el formato aaaa-MM-dd HH:mm.

- **-runasuser runasuser**

  Especifica si se va a cambiar el usuario de la operación de backup programada mientras se programa el backup.

- **-tasktaskspec**

  Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Debe proporcionarse la ruta completa del archivo XML, que proporciona la opción -taskspec .

El comando smo Storage list

Puede ejecutar el comando Storage list para mostrar la lista de sistemas de almacenamiento asociados con un perfil en particular.

Sintaxis

```
        smo storage list
-profile profile
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. El nombre puede tener hasta 30 caracteres y debe ser único dentro del

host.

Ejemplo

En el siguiente ejemplo se muestran los sistemas de almacenamiento asociados al perfil mjulian:

```
smo storage list -profile mjullian
```

```
Sample Output:
Storage Controllers
--------------------
FAS3020-RTP07OLD
```

El comando smo Storage rename

Este comando actualiza el nombre o la dirección IP del sistema de almacenamiento.

Sintaxis

```
        smo storage rename
-profile profile
-oldname old_storage_name
-newname new_storage_name
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-oldname old_storage_name**

  Especifica la dirección IP o el nombre del sistema de almacenamiento antes de cambiar el nombre del sistema de almacenamiento. Debe introducir la dirección IP o el nombre del sistema de almacenamiento que se muestra cuando se ejecuta el comando smo Storage list.

- **-newname new_storage_name**

  Especifica la dirección IP o el nombre del sistema de almacenamiento después de cambiar el nombre del sistema de almacenamiento.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se utiliza el comando smo Storage rename para cambiar el nombre del sistema de almacenamiento:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

El comando dump del sistema de smo

Puede ejecutar el comando system dump para crear un archivo JAR que contenga información de diagnóstico acerca del entorno del servidor.

Sintaxis

```
        smo system dump
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo del comando system dump

En el ejemplo siguiente se utiliza el comando dump del sistema de smo para crear un archivo JAR:

```
smo system dump
Path:/userhomedirectory/.netapp/smo/3.3.0/smo_dump_hostname.jar
```

El comando smo system verify

Este comando confirma que todos los componentes del entorno necesario para ejecutar SnapManager están configurados correctamente.

Sintaxis

```
        smo system verify
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo del comando system verify

En el ejemplo siguiente se usa el comando smo system verify.

```
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.
```

El comando version de smo

Puede ejecutar el comando version para determinar qué versión de SnapManager va a ejecutar en el host local.

Sintaxis

```
        smo version
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra la fecha de creación y el contenido de cada perfil. También muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo del comando version

En el siguiente ejemplo, se muestra la versión de SnapManager:

```
smo version
SnapManager for Oracle Version: 3.3.1
```

Resolución de problemas de SnapManager

Puede encontrar información sobre algunos de los problemas más comunes que se pueden producir y el modo en que puede resolverlos.

La siguiente tabla describe los problemas comunes y las posibles soluciones:

Pregunta basada en cuestiones	Posible solución
¿Se están ejecutando la base de datos de destino y el listener?	Ejecute el comando lsnrctl status. Asegúrese de que la instancia de base de datos está registrada en el listener.
¿El almacenamiento está visible?	Ejecute el comando SnapDrive Storage show -all.
¿Es el almacenamiento editable?	Edite un archivo en el punto de montaje que acaba de crear. Utilice el comando Touch filename. Si se crea el archivo, se puede escribir en el almacenamiento. Debe asegurarse de que el usuario pueda escribir el almacenamiento SnapManager como (por ejemplo, como raíz en UNIX).
¿Se ejecuta el servidor SnapManager?	Ejecute el estado de smo_Server e intente iniciar el servidor mediante el comando start smo_Server. Para poder utilizar la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) para iniciar comandos de la SnapManager relacionados con los perfiles, el servidor debe estar en ejecución. Puede crear o actualizar repositorios sin iniciar el servidor, pero para ejecutar todas las demás operaciones de SnapManager, el servidor debe estar en ejecución. Para iniciar el servidor SnapManager, introduzca el siguiente comando: SMO_Server start.
¿Son todos los componentes necesarios para ejecutar la configuración correcta de SnapManager?	Ejecute el comando smo system verify para comprobar que SnapDrive está configurado correctamente.
¿Tiene la versión correcta de SnapManager?	Use el comando version de smo para comprobar la versión de SnapManager.

Pregunta basada en cuestiones	Posible solución
¿Ha consultado los archivos de registro de SnapManager para determinar si los mensajes de error pueden ayudar a aislar el problema?	SnapManager registra todas las entradas de registro en un conjunto de archivos de registro giratorios. Los archivos de registro se encuentran en /var/log/smo. Los archivos de registro se encuentran en C:\Program_files\NetApp\SnapManager para Oracle\logs. También puede ser útil consultar los registros en la siguiente ubicación: /usr_home/.netapp/smo/3.3.0/log/ Cada registro de operaciones se escribe en su propio archivo de registro con el formato smo_of_date_time.log.
Si tiene registros de archivos almacenados en un sistema de almacenamiento que no ejecuta Data ONTAP, ¿los ha excluido de tener en cuenta para backup con SnapManager?	El archivo smo.config permite excluir determinados archivos de registro de archivos. Para UNIX, los ficheros se encuentran en la siguiente ubicación: /Opt/NetApp/smo/properties/smo.config Utilice el formato mencionado en el archivo para excluir los registros de archivo locales. Para obtener información adicional, consulte el tema "Configuración de propiedades de configuración". También puede excluir los destinos del registro de archivos mientras crea un backup desde la interfaz de línea de comandos de SnapManager. Para obtener información adicional, consulte el tema «"creación de copias de seguridad de bases de datos". También puede excluir los destinos del registro de archivos al crear un backup desde la interfaz gráfica de usuario de SnapManager.
¿Tiene una licencia de FlexClone si utiliza SnapManager con bases de datos de NFS?	Se requiere una licencia de FlexClone para aprovechar al máximo SnapManager con las bases de datos NFS. SnapManager utiliza la función FlexClone para realizar estas tareas: • Montar backups de bases de datos NFS • Verificar backups de bases de datos NFS • Clonar bases de datos NFS • Registrar backups de bases de datos NFS con RMAN (si se utiliza RMAN)

Pregunta basada en cuestiones	Posible solución
¿No ha podido conectarse al repositorio?	Si la conexión a un repositorio falla, ejecute el comando lsnrctl status en la base de datos del repositorio y compruebe los nombres de servicio activos. Cuando SnapManager se conecta a la base de datos del repositorio, utiliza el nombre de servicio de la base de datos. Dependiendo de cómo esté configurado el listener, este puede ser el nombre corto del servicio o el nombre completo del servicio. Cuando SnapManager se conecta a una base de datos para una operación de backup, restauración u otra, utiliza el nombre de host y el SID. Si el repositorio no se inicializa correctamente porque no se puede acceder a él actualmente, recibe un mensaje de error que le pregunta si desea quitar el repositorio. Es posible quitar el repositorio de la vista actual para poder realizar operaciones en otros repositorios. Asimismo, compruebe si la instancia del repositorio se está ejecutando ejecutando ps -eaf
comando grepinstance - name.	¿El sistema puede resolver el nombre de host?
Compruebe si el nombre de host especificado está en una subred diferente. Si recibe un mensaje de error indicando que SnapManager no puede resolver el nombre de host, añada el nombre de host en el archivo de host.Agregue el nombre de host al archivo ubicado en /etc/hosts: xxx.xxx.xxx.xxx.xxx dirección IP	¿Se ejecuta SnapDrive?
Compruebe si el daemon SnapDrive se está ejecutando: -Snapdrived status Si el daemon no se está ejecutando, aparece un mensaje que indica que hay un error de conexión.	¿A qué sistemas de almacenamiento se ha configurado para acceder mediante SnapDrive?
Ejecute el comando: -SnapDrive config list	¿Cómo se puede mejorar el rendimiento de la interfaz gráfica de usuario de SnapManager?

Pregunta basada en cuestiones	Posible solución
• Asegúrese de tener credenciales de usuario válidas para el repositorio, el host de perfiles y el perfil. Si la credencial no es válida, borre las credenciales de usuario para el repositorio, el host del perfil y el perfil. Restablezca las mismas credenciales de usuario que haya establecido antes para el repositorio, el host del perfil y el perfil. Para obtener información adicional acerca de cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales después de borrar la caché de credenciales". • Cierre los perfiles no utilizados. Si el número de perfiles que ha abierto es mayor, el rendimiento de la interfaz gráfica de usuario de SnapManager se ralentiza. • Compruebe si ha activado **Abrir al inicio** en la ventana Preferencias del usuario en el menú **Admin** desde la GUI de SnapManager. Si esto está habilitado, el archivo de configuración de usuario (user.config) disponible en /root/.netapp/smo/3.3.0/gui/state se muestra como openOnStartup=PROFILE. Debido a que **Abrir al inicio** está activado, debe buscar perfiles abiertos recientemente desde la GUI de SnapManager, utilizando lastOpenProfiles en el archivo de configuración de usuario (user.config): LastOpenProfiles=PROFILE1,PROFILE2,PROFILE3,… Puede eliminar los nombres de perfil que aparecen y mantener siempre un número mínimo de perfiles abiertos. • El perfil protegido tarda más tiempo en actualizarse que el perfil que no está protegido. El perfil protegido se actualiza en un intervalo de tiempo, según el valor especificado en el parámetro protectionStatusRefreshRate del archivo de configuración de usuario (user.config). Puede aumentar el valor desde el valor predeterminado (300 segundos) para que los perfiles protegidos se actualicen sólo después del intervalo de tiempo especificado. Antes de instalar la nueva versión de SnapManager en el entorno basado en UNIX, elimine las entradas del cliente de SnapManager	La interfaz gráfica de usuario de SnapManager tarda más tiempo en actualizarse cuando se SnapManager inician y se ejecutan simultáneamente en segundo plano. Al hacer clic con el botón derecho en el backup (que ya se ha eliminado pero se sigue mostrando en la interfaz gráfica de usuario de SnapManager), las opciones de backup para ese backup no se habilitan en la ventana Backup o Clone.

Pregunta basada en cuestiones	Posible solución
Debe esperar hasta que se actualice la interfaz gráfica de usuario de SnapManager y, a continuación, comprobar el estado de backup.	¿Qué haría si la base de datos de Oracle no está configurada en inglés?
Posibilidad de error en las operaciones de SnapManager si el idioma de una base de datos de Oracle no está configurado en inglés. Defina el idioma de la base de datos Oracle en inglés: 1. Añada lo siguiente en los comentarios iniciales en /etc/init.d/smo_Server ◦ NLS_Lang=American_America ◦ Exportar NLS_Lang 2. Reinicie el servidor SnapManager con el siguiente comando: SMO_Server Restart Si las secuencias de comandos de inicio de sesión, como .bash_profile, .bashrc y .cshrc para el usuario de Oracle están definidas en NLS_Lang, debe editar el script para no sobrescribir NLS_Lang.	¿Qué se haría si se produce un error en la operación de programación de backups si la base de datos del repositorio apunta a más de una IP y cada IP tiene un nombre de host diferente?
1. Detenga el servidor SnapManager. 2. Elimine los archivos de programación del directorio de repositorios de los hosts en los que desea activar la programación de backup. Los nombres de los archivos de programación pueden tener los siguientes formatos: ◦ repository#repo_username#repository_database_name#repository_host#repo_port ◦ Repository-repo_usernamereppository_database_name-repository_host-repo_Port **Nota:** debe asegurarse de que elimine el archivo de programa en el formato que coincida con los detalles del repositorio. 3. Reinicie el servidor SnapManager. 4. Abra otros perfiles en el mismo repositorio de la interfaz gráfica de usuario de SnapManager para asegurarse de que no se pierda ninguna información de programación de dichos perfiles.	¿Qué haría si la operación de SnapManager presenta un error de bloqueo del archivo de credenciales?

Pregunta basada en cuestiones	Posible solución
SnapManager bloquea el archivo de credenciales antes de la actualización y lo desbloquea después de la actualización.cuando se ejecutan varias operaciones a la vez, una de las operaciones puede bloquear el archivo de credenciales para actualizarlo. Si otra operación intenta acceder al archivo de credenciales bloqueadas al mismo tiempo, la operación genera un error de bloqueo de archivo. Configure los siguientes parámetros en el archivo smo.config en función de la frecuencia de las operaciones simultáneas: • FileLock.RetryInterval = 100 milisegundos • FileLock.timeout = 5000 milisegundos Los valores asignados a los parámetros deben ser en milisegundos.	¿Qué haría si el estado intermedio de la operación de verificación de backup muestra un error en la pestaña Monitor aunque todavía esté en ejecución la operación de verificación de backup?

El mensaje de error se registra en el archivo sm_gui.log. Debe buscar en el archivo de registro para determinar los nuevos valores de operation.heartbeatInterval and operation.heartbeatThreshold que resolverán este problema.
 	
1. Añada los siguientes parámetros en el archivo smo.config:
  ◦ Operation.heartbeatInterval = 5000
  ◦ Operation.heartbeatThreshold = 5000 el valor predeterminado asignado por SnapManager es 5000.
2. Asigne nuevos valores a estos parámetros.
 	
Los valores asignados a los parámetros deben ser en milisegundos.
 	
3. Reinicie el servidor SnapManager y vuelva a realizar la operación.
	¿Qué se debe hacer cuando se encuentra un problema de espacio en montón?

Pregunta basada en cuestiones	Posible solución
Cuando encuentre un problema de espacio en montón durante las operaciones de SnapManager para Oracle, debe realizar los siguientes pasos: 1. Desplácese hasta el directorio de instalación de SnapManager para Oracle. 2. Abra el archivo Launchjava desde la ruta installationdirectory/bin/Launchjava. 3. Aumente el valor del parámetro java -Xmx160m Java heap-space. Por ejemplo, puede aumentar el valor predeterminado de 160 m a 200 m. Si ha aumentado el valor del parámetro Java heap-space en las versiones anteriores de SnapManager para Oracle, debe conservar ese valor.	¿Qué haría si no pudiera utilizar los backups protegidos para restaurar o clonar?
Este problema se observa si utiliza SnapManager 3.3.1 con Clustered Data ONTAP y se ha actualizado a SnapManager 3.4. Los backups se protegieron mediante secuencias de comandos posteriores en SnapManager 3.3.1. A partir de SnapManager 3.4, los backups se protegen con las políticas *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault* que se seleccionan al crear un perfil.después de actualizar a SnapManager 3.4, es posible que siga utilizando los perfiles antiguos y, por lo tanto, los backups se protejan con scripts de backup, Pero no puede usarlos para restaurar o clonar mediante SnapManager. Debe actualizar el perfil y seleccionar la política *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault* y eliminar el script posterior que se utilizó para la protección de datos en SnapManager 3.3.1.	¿Qué haría si los backups programados no se protegerían (SnapVault)?

Volcar archivos

Los archivos de volcado son archivos de registro comprimidos que contienen información acerca de SnapManager y su entorno. Los diferentes tipos de archivos de registro creados son operación, perfil y archivo de volcado del sistema.

Puede utilizar el comando dump o la ficha **Create Diagnostics** de la interfaz gráfica de usuario (GUI) para recopilar información sobre una operación, un perfil o el entorno. Un volcado del sistema no requiere un perfil;

sin embargo, los volcados de perfil y operación requieren perfiles.

SnapManager incluye la siguiente información de diagnóstico en el archivo de volcado:

- Los pasos realizados
- El tiempo que tarda cada paso en completarse
- El resultado de cada paso
- Error, si hay alguno, que ocurrió durante la operación

> Los archivos de registro o los archivos de volcado de SnapManager permiten permisos de lectura y escritura sólo para los usuarios raíz y los demás usuarios que pertenecen al grupo de usuarios raíz.

SnapManager también incluye la siguiente información en el archivo:

- Arquitectura y versión del sistema operativo
- Variables de entorno
- Versión de Java
- Arquitectura y versión de SnapManager
- Preferencias de SnapManager
- Mensajes de SnapManager
- propiedades log4j
- Arquitectura y versión de SnapDrive
- Archivos de registro de SnapDrive
- Versión de Oracle
- Detalles del inventario local de Oracle OPatch
- Detalles del inventario local de OPatch de la instancia de Automatic Storage Management (ASM)
- Versión del sistema de almacenamiento
- Archivo oratab de Oracle
- Estado del listener de Oracle
- Archivos de configuración de red de Oracle (listener.ora y tnsnames.ora)
- Versión de Oracle de la base de datos del repositorio
- Tipo de base de datos de destino (clústeres de aplicaciones reales (RAC) o en soporte)
- Función de base de datos de destino (primaria, física en espera o lógica en espera)
- Configuración de Oracle Recovery Manager (RMAN) de la base de datos de destino (sin integración de RMAN, RMAN con archivos de control o RMAN con archivo de catálogo)
- Versión de la instancia de ASM de la base de datos de destino
- Versión de Oracle de la base de datos de destino
- Identificador del sistema (SID) de la base de datos de destino
- Nombre de la base de datos RMAN y nombre de la conexión TNS
- Nombre del servicio de base de datos del repositorio

- Instancias de base de datos instaladas en el host
- Descriptor perfil
- Memoria compartida máxima
- Intercambie información de espacio
- Información de la memoria
- Versión del kernel
- FSTAB
- Protocolo que utiliza SnapDrive
- Entorno multivía
- RAC
- Gestor de volúmenes admitido
- Versión de Operations Manager
- Sistema de archivos compatible
- Versión de utilidades de host
- Resultado del comando system verify
- Resultado del comando sdconfcheck

Los archivos de volcado de SnapManager también contienen el archivo de recopilador de datos de SnapDrive y el archivo de registro de alertas de Oracle. Puede recopilar el archivo de registro de alertas de Oracle mediante los comandos de volcado de la operación smo y de volcado de perfiles de smo.

> El volcado del sistema no contiene registros de alertas de Oracle; sin embargo, los volcados de alerta y de operación contienen los registros de alerta.

Aunque no se esté ejecutando el servidor host SnapManager, puede acceder a la información de volcado mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario.

Si se encuentra con un problema que no se puede resolver, puede enviar estos archivos a los servicios globales de NetApp.

Creación de archivos de volcado en el nivel de las operaciones

Puede utilizar el comando de volcado de la operación de smo con el nombre o el ID de la operación fallida para obtener información del registro sobre una operación en particular. Es posible especificar niveles de registro diferentes para recopilar información sobre una operación, un perfil, un host o un entorno específicos.

1. Introduzca el siguiente comando: Volcado de operación de smo -idguid

   > El comando smo operation dump proporciona un superconjunto de la información proporcionada por el comando de volcado de perfil de smo, que a su vez proporciona un superconjunto de la información proporcionada por el comando de volcado del sistema smo.

   Ubicación del archivo de volcado:

```
Path:/<user-home>
/.netapp/smo/3.3.0/smo_dump_8abc01c814649ebd0114649ec69d0001.jar
```

Creación de archivos de volcado a nivel de perfil

Puede encontrar información de registro sobre un perfil determinado mediante el comando smo profile dump con el nombre del perfil.

1. Introduzca el siguiente comando: Volcado de perfil de smo -profile profile profile_name

   Ubicación del archivo de volcado:

   ```
   Path:/<user-home>
   /.netapp/smo/3.3.0/smo_dump_8abc01c814649ebd0114649ec69d0001.jar
   ```

   > Si se produce un error al crear un perfil, utilice el comando smosystem dump. Una vez que haya creado correctamente un perfil, utilice los comandos de volcado de operación smooperation y de volcado de moporofile.

Creación de archivos de volcado en el nivel del sistema

Puede usar el comando de volcado del sistema smo para obtener información sobre el registro del entorno y el host de SnapManager. Es posible especificar niveles de registro diferentes para recoger información sobre una operación, un perfil o un host y un entorno específicos.

1. Introduzca el siguiente comando: Volcado de sistema smo

   Volcado resultante

   ```
   Path:/<user-home>/.netapp/smo/3.3.0/smo_dump_server_host.jar
   ```

Cómo localizar archivos de volcado

El archivo de volcado se encuentra en el sistema cliente para facilitar el acceso. Estos archivos son útiles si necesita solucionar un problema relacionado con el perfil, el sistema o cualquier operación.

El archivo de volcado se encuentra en el directorio principal del usuario en el sistema cliente.

- Si utiliza la interfaz gráfica de usuario (GUI), el archivo de volcado se encuentra en:

```
user_home/Application Data/NetApp/smo/3.3.0/smo_dump dump_file_type_name
server_host.jar
```

- Si utiliza la interfaz de línea de comandos (CLI), el archivo de volcado se encuentra en:

```
user_home/.netapp/smo/3.3.0/smo_dump_dump_file_type_name server_host.jar
```

El archivo dump contiene el resultado del comando dump. El nombre del archivo depende de la información proporcionada. En la siguiente tabla se muestran los tipos de operaciones de volcado y los nombres de archivo resultantes:

Tipo de operación de volcado	Nombre de archivo resultante
Comando de volcado de la operación con ID de operación	smo_dump_operation-id.jar

Comando de volcado de la operación sin ID de operación	Se muestra la siguiente salida de volcado de la operación de smo -profile VH1-verbose:
	`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`

Comando system dump	smo_dump_host-name.jar
Comando de volcado de perfil	smo_dump_profile-name_host-name.jar

Cómo recopilar archivos de volcado

Es posible incluir -dump en el comando SnapManager para recoger los archivos de volcado después de una operación de SnapManager correcta o con errores.

Es posible recoger archivos de volcado para las siguientes operaciones de SnapManager:

- Creación de perfiles
- Actualizando perfiles

- Crear backups
- Verificación de backups
- Eliminar backups
- Liberando backups
- Montar backups
- Desmontaje de backups
- Restaurar backups
- Crear clones
- Eliminar clones
- Dividir clones

> Al crear un perfil, puede recopilar archivos de volcado sólo si la operación se realiza correctamente. Si se produce un error al crear un perfil, debe utilizar el comando de volcado del sistema smsystem. Para que los perfiles se realicen correctamente, puede utilizar los comandos de volcado smooperation y smoprofile para recopilar los archivos de volcado.

ejemplo

```
      smo  backup create -profile targetdb1_prof1 -auto -full -online
-dump
```

Recopilación de información de registro adicional para facilitar la depuración

Si necesita registros adicionales para depurar una operación de SnapManager con errores, debe configurar una variable de entorno externa Server.log.level. Esta variable anula el nivel de registro predeterminado y vuelca todos los mensajes de registro del archivo de registro. Por ejemplo, puede cambiar el nivel de registro a DEBUG, lo que registra mensajes adicionales y puede ayudar en la depuración de problemas.

Los registros de SnapManager se pueden encontrar en las siguientes ubicaciones:

- /var/log/smo

Para anular el nivel de registro predeterminado, debe realizar los siguientes pasos:

1. Cree un archivo de texto platform.override en el directorio de instalación de SnapManager.
2. Agregue el parámetro Server.log.level en el archivo de texto platform.override.
3. Asignar un valor (SEGUIMIENTO, DEPURACIÓN, INFO, WARN, ERROR, FATAL o PROGRESS) en el parámetro Server.log.level.

   Por ejemplo, para cambiar el nivel de registro a ERROR, establezca el valor Server.log.level en ERROR.

   Server.log.level=ERROR

4. Reinicie el servidor SnapManager.

Si no se necesita la información adicional del registro, puede eliminar el parámetro Server.log.level del archivo de texto platform.override.

SnapManager gestiona el volumen de archivos de registro del servidor según los valores definidos por el usuario de los siguientes parámetros en el archivo smo.config:

- log.max_log_files
- log.max_log_file_size
- log.max_rolling_operation_factory_logs

Solucionar problemas de clones

Puede encontrar información sobre eso que puede ocurrir durante las operaciones de clonado y cómo puede resolverla.

Síntoma	Explicación	Solución alternativa
Se produce un error en la operación de clonado cuando el destino de archivado está establecido en USE_DB_RECOVERY_FILE_DEST.	Cuando el destino de archivado hace referencia a USE_DB_RECOVERY_FILE_DEST, el área de recuperación flash (FRA) gestiona activamente el registro de archivos. SnapManager no utiliza la ubicación de la FRA durante las operaciones de clonado o restauración y, por lo tanto, fallan las operaciones.	Cambie el destino de archivado por la ubicación del registro de archivos real en lugar de la ubicación del FRA.

Síntoma	Explicación	Solución alternativa
Se produce un error en la operación de clonado con el siguiente mensaje de error: Cannot Perform: Clone Create. Causa raíz: ORACLE-00001: Error al ejecutar SQL: [ALTER DATABASE OPEN RESETLOGS;]. El comando devolvió: ORA-01195: El backup en línea del archivo 1 necesita más recuperación para ser coherente.	Este problema ocurre si Oracle listener no puede conectarse a la base de datos.	Si utiliza la interfaz gráfica de usuario de SnapManager para clonar un backup, realice las siguientes acciones: 1. En el árbol del repositorio, haga clic en **repositorio** > **Host** > **Perfil** para visualizar las copias de seguridad. 2. Haga clic con el botón derecho del ratón en la copia de seguridad que desea clonar y seleccione **Clonar**. 3. En la página Clone Initialization, introduzca los valores obligatorios y seleccione el método de especificación del clon. 4. En la página Clone Specification, seleccione **parámetros**. 5. Haga clic en la ficha **+parámetro**. 6. En el campo **Nombre de parámetro**, introduzca el nombre como local_listener y haga clic en **Aceptar**. 7. Active la casilla de verificación **Anular valor predeterminado** de la fila local_listener. 8. Haga clic en cualquier parámetro y, a continuación, haga doble clic en el parámetro local_listener e introduzca el siguiente valor:(ADDRESS=(PROTOCOL=TCP)(HOST=<your_host_name>)(PORT=<port#>))) 9. Haga clic en **Guardar en archivo**. 10. Haga clic en **Siguiente** y continúe con el asistente de creación de clones. Si está utilizando CLI para clonar una copia de seguridad, debe incluir la siguiente información en la etiqueta **<parameters>** del archivo de especificación del clon:

Síntoma	Explicación	Solución alternativa
Se produce un error en la operación de clonado con un mensaje de error que indica que el punto de montaje que está usando ya está en uso.	SnapManager no permite montar un clon en un punto de montaje existente. Por lo tanto, un clon incompleto no eliminaba el punto de montaje.	Especifique otro punto de montaje para que lo utilice el clon, o desmonte el punto de montaje problemático.
Se produce un error en la operación de clonado con un mensaje de error acerca de los archivos de datos que no tienen la extensión .dbf.	Algunas versiones de la utilidad Oracle NID no funcionan con archivos de datos a menos que los archivos utilicen una extensión .dbf.	• Cambie el nombre del archivo de datos para darle una extensión .dbf. • Repita la operación de backup. • Clone el backup nuevo.
Se produce un error en la operación de clonado debido a requisitos no cumplidos.	Está intentando crear un clon; sin embargo, no se cumplieron algunos de los requisitos previos.	Proceda como se describe en *creando un clon* para cumplir con los requisitos previos.
SnapManager no logra generar un nuevo perfil después de la operación de división de clones y el usuario no sabe si se crea el nuevo perfil.	SnapManager no puede preguntar si no se crea un nuevo perfil después de la operación de división de clones. Dado que no se muestra el mensaje, puede suponer que se crea el perfil.	En la interfaz de línea de comandos (CLI) de SnapManager, introduzca el comando clone split-result para ver el resultado detallado de la operación de división de clones.
SnapManager para Oracle no puede clonar bases de datos físicas de Oracle 10gR2 (10.2.0.5) en espera de Oracle Data Guard.	SnapManager para Oracle no deshabilita el modo de recuperación gestionado mientras se realiza un backup sin conexión de las bases de datos físicas en espera de Oracle 10gR2 (10.2.0.5) creadas con los servicios de Oracle Data Guard. Debido a este problema, el backup sin conexión realizado no es coherente. Cuando SnapManager para Oracle intenta clonar el backup sin conexión, ni siquiera intenta realizar una recuperación en la base de datos clonada. Como el backup no es coherente, la base de datos clonada requiere una recuperación y, por lo tanto, Oracle no puede crear el clon correctamente.	Actualización de la base de datos Oracle a Oracle 11gR1 (parche 11.1.0.7).

Síntoma	Explicación	Solución alternativa
Se produce un error en la clonado de un backup en un host remoto con el siguiente mensaje de error: Se deniega el acceso.	Durante el montaje, si la dirección IP del host se proporciona al comando de montaje Snap, se podría producir un error en la operación de clonado. Este problema ocurre si el host en el que reside la base de datos está en el grupo de trabajo mientras el host remoto está en el dominio o viceversa.	Debe asegurarse de que tanto el host remoto como el host en el que reside la base de datos están en el dominio y no en el grupo de trabajo.

Solución de problemas de la interfaz gráfica de usuario

Es posible encontrar información sobre algunos problemas de la interfaz gráfica de usuario (GUI) conocidos comunes que pueden ser de ayuda para resolverlos.

Problema	Explicación	Solución alternativa
Al acceder a la GUI de SnapManager para realizar una operación, puede aparecer el siguiente mensaje de error: SMO-20111 : error de autenticación para el usuario en el host.	Este problema se produce si se cambia la contraseña del usuario en el host en el que se ejecuta el servidor SnapManager.después de cambiar la contraseña, la caché de credenciales creada para el usuario que inició la GUI deja de ser válida. La interfaz gráfica de usuario de SnapManager sigue utilizando las credenciales de la caché para autenticar y, por lo tanto, la autenticación falla.	Debe realizar una de las siguientes tareas: • Elimine las credenciales del usuario cuya contraseña se modificó y añada las nuevas credenciales en la caché ejecutando los siguientes comandos: a. eliminación de la credencial de smo b. se han establecido credenciales de smo • Borrar toda la caché ejecutando el comando clear de credenciales de smo. Vuelva a abrir la GUI y establezca las credenciales, si se le solicita.
Se muestra una advertencia de seguridad mientras se utiliza Java Web Start para acceder a la GUI de SnapManager.	Al acceder a la GUI de SnapManager mediante Java Web Start, se muestra una advertencia de seguridad.este problema se produce porque los tarros JNLP son autofirmados y la versión Java utilizada por SnapManager no permite los tarros autofirmados en un nivel de seguridad alto.	Cambie la configuración de seguridad a medio en el panel de control de Java o agregue la dirección URL de la GUI de SnapManager a la lista de excepciones.

Problema	Explicación	Solución alternativa
La interfaz gráfica de usuario de inicio web de SnapManager muestra la versión incorrecta.	Después de cambiar a SnapManager de una versión posterior a una versión anterior al iniciar la GUI de inicio web, se inicia la versión posterior de la GUI de inicio web de SnapManager.	También debe borrar la caché realizando los siguientes pasos: 1. Inicie la consola. 2. Introduzca lo siguiente: Javaws -viewer 3. En la pantalla del visor de caché Java, haga clic con el botón derecho del ratón en la aplicación SnapManager y seleccione **Eliminar**.
Al reiniciar la GUI e intentar comprobar las copias de seguridad de un perfil determinado, sólo verá los nombres de los perfiles.	SnapManager no muestra ninguna información sobre un perfil hasta que lo abre.	Siga estos pasos: 1. Haga clic con el botón derecho del ratón en el perfil y seleccione **Abrir** en el menú. SnapManager muestra el cuadro de diálogo autenticación de perfiles. 2. Introduzca el nombre de usuario y la contraseña del host. SnapManager muestra la lista de backups. Sólo es necesario autenticar el perfil una vez, siempre que las credenciales sean válidas y permanezcan en la caché.
Al abrir el primer repositorio en la GUI, aparece un mensaje de error similar al siguiente: El nombre de perfil XXXX choca con el repositorio cargado previamente.	Los perfiles con el mismo nombre no pueden existir en un repositorio. Además, solo es posible abrir un repositorio a la vez.	Haga referencia a los perfiles en conflicto de dos usuarios de sistema operativo (SO) diferentes o cambie el nombre del perfil emitiendo una sentencia SQL para el repositorio: ACTUALIZAR SMO_33_PROFILE SET NAME = 'NEW_NAME' DONDE NAME = 'OLD_NAME'

Problema	Explicación	Solución alternativa
Se muestra un mensaje de error similar al siguiente: SMO-01092: No se puede inicializar la repo1@ del repositorio no existe:repo1SMO-11006: No se puede resolver el host no existe	El repositorio es inaccesible, quizás porque ya no existe. La GUI inicializa la lista de repositorios desde el archivo de credenciales.	El mensaje de error le pregunta si desea eliminar este repositorio para que no se intente cargarlo en el futuro. Si no necesita acceder a este repositorio, haga clic en **Eliminar** para eliminarlo de la vista GUI. Esto elimina la referencia al repositorio en el archivo de credenciales y la interfaz gráfica de usuario no intenta volver a cargar el repositorio.

La creación de perfiles falla porque las credenciales de host no se autentican en las plataformas SUSE Linux Enterprise Server 10 y SUSE Linux Enterprise Server 11.	SnapManager utiliza el módulo de autenticación conectable (PAM) para autenticar usuarios. En las plataformas 10 y 11 de SUSE Linux Enterprise Server, no hay ningún archivo SnapManager de forma predeterminada en el directorio /etc/pam.d que proporcione los detalles de autenticación necesarios. De este modo, se producen errores en las credenciales del host.	Para iniciar sesión correctamente en el host de las plataformas SUSE Linux Enterprise Server 10 y 11, realice los siguientes pasos:
		1. Cree un archivo SnapManager en /etc/pam.d/.
		2. Añada el siguiente contenido al archivo SnapManager ubicado en /etc/pam.d/snapmanager:
		`#%PAM-1.0`
		`auth include common-auth`
		`account include common-account`
		`password include common-password`
		`session include common-session`
		3. Guarde el archivo y vuelva a intentar la operación de creación de perfiles.

Problema	Explicación	Solución alternativa
SnapManager tarda más tiempo en cargar la estructura del árbol de la base de datos y da como resultado un mensaje de error de tiempo de espera que se muestra en la interfaz gráfica de usuario de SnapManager.	Cuando se intenta realizar una operación de backup parcial desde la interfaz gráfica de usuario de SnapManager, SnapManager intenta cargar las credenciales para todos los perfiles y, si hay entradas no válidas, SnapManager intenta validar la entrada y esto provoca que se muestre un mensaje de error de tiempo de espera.	Elimine las credenciales del host, el repositorio y el perfil que no utilice el comando credential delete de la interfaz de línea de comandos (CLI) de SnapManager.
SnapManager no logra generar un nuevo perfil después de la operación de división de clones y no sabe si se crea el nuevo perfil.	SnapManager no puede preguntar si no se crea un nuevo perfil después de la operación de división de clones. Dado que no se muestra ningún mensaje para la operación fallida, puede suponer que se crea el perfil.	Para saber si se crea un nuevo perfil para la operación de división de clones, realice los siguientes pasos: 1. Haga clic en la ficha **Monitor**, haga clic con el botón derecho del ratón en la entrada de la operación de división de clones y seleccione **Propiedades**. 2. En la ventana Propiedades del perfil, haga clic en la ficha **registros** para ver la operación de división de clones y los registros de creación de perfiles.
Los scripts personalizados para el procesamiento previo o posterior a la actividad que se realizan antes o después de las operaciones de backup, restauración o clonado no se pueden ver en la interfaz gráfica de usuario de SnapManager.	Cuando se añaden scripts personalizados en la ubicación del backup, la restauración o la clonado de scripts después de iniciar el asistente respectivo, los scripts personalizados no se muestran en la lista Available Scripts.	Reinicie el servidor host SnapManager y, a continuación, abra la interfaz gráfica de usuario de SnapManager.
No se puede utilizar el archivo XML de especificación del clon creado en SnapManager (3.1 o anterior) para la operación de clonado.	Desde SnapManager 3.2 para Oracle, la sección de especificación de tareas (especificación de tareas) se proporciona como un archivo XML de especificación de tareas independiente.	Si utiliza SnapManager 3.2 para Oracle, debe eliminar la sección de especificación de tareas del XML de especificación del clon o crear un archivo XML de especificación del clon nuevo.SnapManager 3.3 o posterior no admite el archivo XML de especificación del clon creado en SnapManager 3.2 o versiones anteriores.

Problema	Explicación	Solución alternativa
El funcionamiento de SnapManager en la GUI no se realiza después de haber borrado las credenciales de usuario mediante el comando smo credential clear desde la CLI de SnapManager o haciendo clic en **Admin** > **credenciales** > **Borrar** > **caché** desde la interfaz gráfica de usuario de SnapManager.	Se borran las credenciales establecidas para los repositorios, hosts y perfiles. SnapManager verifica las credenciales de usuario antes de iniciar cualquier operación.cuando las credenciales de usuario no son válidas, SnapManager no puede autenticarse. Cuando se elimina un host o un perfil del repositorio, las credenciales del usuario siguen estando disponibles en la caché. Estas entradas de credenciales innecesarias ralentizan las operaciones de SnapManager de la interfaz gráfica de usuario.	Reinicie la interfaz gráfica de usuario de SnapManager en función de cómo se borre la caché. **Nota:** • Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager. • Si borró la caché de credenciales de la interfaz gráfica de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager. • Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar la interfaz gráfica de usuario de SnapManager. Configure las credenciales que haya otorgado para el repositorio, el host del perfil y el perfil. Desde la GUI de SnapManager, si no hay ningún repositorio asignado en el árbol de repositorios, realice los siguientes pasos: 1. Haga clic en **tareas** > **Agregar repositorio existente** 2. Haga clic con el botón derecho del ratón en el repositorio, haga clic en **Abrir** e introduzca las credenciales de usuario en la ventana **autenticación de credenciales de repositorio**. 3. Haga clic con el botón derecho del ratón en el host bajo el repositorio, haga clic en **Abrir** e introduzca las credenciales de usuario en **autenticación de credenciales de host**. 4. Haga clic con el botón derecho del ratón en el perfil bajo el host, haga clic en **Abrir** e introduzca las credenciales de usuario en **autenticación de credenciales de perfil**.

Problema	Explicación	Solución alternativa
El mensaje de error no puede enumerar las políticas de protección por el siguiente motivo: Protection Manager no está disponible temporalmente se muestra cuando selecciona **Ninguno** en el menú desplegable **Directiva de protección de Protection Manager** de la ventana Propiedades de perfil y la página de configuración de directivas del asistente de creación de perfiles.	Protection Manager no se configuró con SnapManager o Protection Manager no está en ejecución.	No es necesario realizar ninguna acción.
No se puede abrir la GUI de SnapManager mediante la GUI de inicio web de Java debido a la fortaleza del cifrado de capa de sockets seguros (SSL) más débil del explorador.	SnapManager no admite cifrados SSL de más de 128 bits.	Actualice la versión del navegador y compruebe la intensidad del cifrado.

Resolución de problemas de SnapDrive

Puede que tenga algunos problemas comunes al utilizar SnapManager con productos de SnapDrive.

En primer lugar, debe determinar si el problema está relacionado con SnapManager para Oracle o SnapDrive. Si el problema es un error de SnapDrive, SnapManager para Oracle muestra un mensaje de error similar al siguiente:

```
SMO-12111: Error executing snapdrive command "<snapdrive command>":
<snapdrive error>
```

A continuación se muestra un ejemplo de un mensaje de error de SnapDrive en el que SMO-12111 es el número de error de SnapManager. El esquema de numeración 0001-770 representa SnapDrive para los errores UNIX.

```
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.
```

A continuación, se muestran los mensajes de error más comunes de SnapDrive para UNIX relacionados con la detección de LUN, los problemas de configuración y el espacio. Si recibe alguno de estos errores, consulte el capítulo solución de problemas de la *Guía de instalación y administración de SnapDrive*.

Síntoma	Explicación
0001-136 error de administrador: No se puede iniciar sesión en el archivador: <filer> establezca un nombre de usuario y/o una contraseña para <filer>	Configuración inicial de SnapDrive
0001-382 error de administrador: Se ha producido un error en la detección multivía	Error de detección de LUN
0001-462 error de administrador: No se pudo desconfigurar la multivía para <LUN>: Spd5: No se puede detener el dispositivo. Dispositivo ocupado.	Error de detección de LUN
0001-476 error de administrador: No se puede detectar el dispositivo asociado con … 0001-710 error de administrador: Error de actualización del SO de LUN…	Error de detección de LUN
0001-680 error de administrador: El SO del host requiere una actualización de los datos internos para permitir la creación o la conexión de la LUN. Use "SnapDrive config prepare lun" o actualice esta información manualmente…	Error de detección de LUN
0001-817 error de administrador: Error al crear el clon de volumen… : FlexClone no tiene licencia	Configuración inicial de SnapDrive
0001-878 error de administrador: No se ha encontrado el asistente de HBA. Los comandos que implican las LUN deben fallar.	Error de detección de LUN

Solucionar problemas de cambio de nombre del sistema de almacenamiento

Puede enfrentarse a problemas al cambiar el nombre de un sistema de almacenamiento o después de haber cambiado correctamente el nombre del sistema de almacenamiento.

Cuando intenta cambiar el nombre del sistema de almacenamiento, es posible que se produzca un error en la operación con el siguiente mensaje: SMO-05085 no se ha encontrado ninguna controladora de almacenamiento "fas3020-rtp07New" que esté asociada con el perfil

Debe introducir la dirección IP o el nombre del sistema de almacenamiento que aparece cuando ejecuta el comando smo Storage list.

Después de cambiar el nombre del sistema de almacenamiento, es posible que se produzca un error en las operaciones de SnapManager si SnapManager no reconoce el sistema de almacenamiento. Para resolver este problema, debe realizar algunos pasos adicionales en el host del servidor de DataFabric Manager y en el host del servidor SnapManager.

Realice los siguientes pasos en el host del servidor de DataFabric Manager:

1. Eliminar la dirección IP y el host del sistema de almacenamiento anterior en el archivo de host ubicado en /etc/hosts en el host del servidor de DataFabric Manager.
2. Añada la nueva dirección IP y el nuevo host del sistema de almacenamiento en el archivo host ubicado en /etc/hosts en el host del servidor de DataFabric Manager.
3. Cambie el nombre del host de almacenamiento introduciendo el siguiente comando: dfm host rename -a old_host_namenew_host_name
4. Configure la nueva dirección IP en el host. Para ello, introduzca el siguiente comando: dfm host set old_host_name_or_objId hostPrimaryAddress = new_Storage_Controller_ip_address

   > Este paso debe realizarse solo si se especificó la dirección IP como nombre del nuevo sistema de almacenamiento.

5. Actualice el nuevo nombre del sistema de almacenamiento en el host de DataFabric Manager Server. Para ello, introduzca el siguiente comando: dfm host diag old_Storage_name

   Puede verificar si el nombre de la controladora de almacenamiento anterior se reemplaza por un nuevo nombre de la controladora de almacenamiento. Para ello, introduzca el siguiente comando: dfm host Discover new_Storage_name

Realice los siguientes pasos como usuario raíz en el host del servidor SnapManager.

> Cuando se introduce el nuevo nombre de controladora de almacenamiento, se debe utilizar el nombre de alias del sistema y no el nombre de dominio completo (FQDN).

1. Elimine el nombre del sistema de almacenamiento anterior introduciendo el siguiente comando: SnapDrive config delete old_Storage_name

   > Si no elimina el nombre de sistema de almacenamiento anterior, todas las operaciones de SnapManager fallarán.

2. Eliminar la dirección IP y el host del sistema de almacenamiento anterior en el archivo de host ubicado en etc/hosts en el host de la base de datos de destino.

3. Añada la nueva dirección IP y el host del nuevo sistema de almacenamiento en el archivo host ubicado en /etc/hosts en el host de la base de datos de destino.
4. Añada el nombre del nuevo sistema de almacenamiento introduciendo el siguiente comando: SnapDrive config set root new_Storage_name
5. Asigne los nombres de sistema de almacenamiento anteriores y posteriores introduciendo el siguiente comando: SnapDrive config migrate set old_Storage_namenew_Storage_name
6. Elimine la ruta de gestión del sistema de almacenamiento anterior introduciendo el siguiente comando:snapdrive config delete -mgmtpath old_Storage_name
7. Añada la ruta de gestión del nuevo sistema de almacenamiento introduciendo el siguiente comando: SnapDrive config set -mgmtpath new_Storage_name
8. Actualice el conjunto de datos para los archivos de datos y los archivos de registro de archivos con el nuevo nombre del sistema de almacenamiento introduciendo el siguiente comando: SnapDrive dataset changehostname -dndataset_name-oldnamedold_Storage_name-newnamenew_Storage_name
9. Actualice el perfil del nuevo nombre del sistema de almacenamiento introduciendo el siguiente comando: smo Storage rename -profileprofile_name-oldnamold_Storage_name-newnamenew_Storage_name
10. Comprobar el sistema de almacenamiento asociado con el perfil introduciendo el siguiente comando: smo Storage list -profileprofile_name

Resolución de problemas conocidos

Es necesario conocer algunos problemas conocidos que se pueden producir al utilizar SnapManager y cómo solucionar sus problemas.

SnapManager para Oracle no identifica los perfiles de modo Cluster

Si el nombre del perfil de Cluster-Mode no está presente en el archivo cmode_profiles.config del directorio de instalación de SnapManager para Oracle, el siguiente mensaje de error podría activarse:

Configure el servidor DFM mediante la configuración de SnapDrive set -dfm user_name Appliance_name.

Además, al actualizar SnapManager para Oracle, si elimina la carpeta /opt/NetApp/smo/*, el archivo cmode_profiles.config que tiene los nombres de perfil de Cluster-Mode también se elimina. Este problema también activa el mismo mensaje de error.

Solución

Actualice el perfil: <profile_name> de perfil de actualización de smo

> Si se instala SnapManager para Oracle en la ruta /opt/NetApp/smo/, la ubicación del archivo es /opt/NetApp/smo/cmode_profile/cmode_profiles.config.

El servidor no se inicia

Al iniciar el servidor, es posible que aparezca un mensaje de error similar al siguiente:

SMO-01104: Error al invocar el comando: SMO-17107: El servidor SnapManager no se pudo iniciar en el puerto 8074 debido a los siguientes errores: La dirección java.net.BindException: ya está en uso

Esto puede deberse a que los puertos de escucha SnapManager (27214 y 27215, de forma predeterminada) están actualmente en uso en otra aplicación.

Este error también puede ocurrir si el comando smo_Server ya se está ejecutando, pero SnapManager no detecta el proceso existente.

Solución

Es posible volver a configurar SnapManager o la otra aplicación para utilizar diferentes puertos.

Para volver a configurar las SnapManager, edite el siguiente archivo: /Opt/NTAP/smo/properties/smo.config

Asigne los siguientes valores:

- Servidor de SMO.Port=27214
- Servidor SMO.rmiRegistry.Port=27215
- remote.registry.ocijdbc.port= 27215

  El archivo remote.registry.ocijdbc.Port debe ser el mismo que Server.rmiRegistry.Port.

Para iniciar el servidor SnapManager, introduzca el siguiente comando: SMO_Server start

> Si el servidor ya se está ejecutando, aparecerá un mensaje de error.

Si el servidor ya está en ejecución, realice los siguientes pasos:

1. Detenga el servidor introduciendo el siguiente comando: smo_Server stop
2. Para reiniciar el servidor, introduzca el siguiente comando: Inicio smo_Server

Terminando una operación SnapManager en ejecución actualmente

Si el servidor SnapManager se bloquea y no puede ejecutar ninguna operación correctamente, puede finalizar SnapManager y sus operaciones.

Solución

SnapManager funciona tanto con SnapManager como con Protection Manager. Debe realizar los siguientes pasos para enumerar los diferentes procesos en ejecución y detener el último proceso en ejecución.

1. Enumere todos los procesos de SnapDrive que se están ejecutando: ps

   Ejemplo: ps | grep SnapDrive

2. Detenga el proceso o los procesos de SnapDrive: Kill <pid>

   pid es la lista de procesos encontrados mediante el comando ps.

   > No se detienen todos los procesos de SnapDrive. Se recomienda finalizar solo el último proceso en ejecución.

3. Si una de las operaciones implica restaurar un backup protegido desde un almacenamiento secundario, abra la consola de Protection Manager y realice lo siguiente:
   a. En el menú sistema, seleccione **trabajos**.
   b. Seleccione **Restaurar**.

   c. Compruebe el nombre del conjunto de datos que coincide con el del perfil de SnapManager.
   d. Haga clic con el botón derecho del ratón y seleccione **Cancelar**.
4. Enumerar los procesos de SnapManager:
   a. Inicie sesión como usuario root.
   b. Enumerar los procesos mediante el comando ps.

      Ejemplo: ps | grep java
5. Finalizar el proceso de SnapManager: Matar a <pid>

No se puede eliminar ni liberar la última copia de seguridad protegida

Cuando se crea el primer backup para un perfil en el almacenamiento secundario, SnapManager envía toda la información sobre el backup a Protection Manager. Para backups posteriores relacionados con este perfil, SnapManager solo envía la información modificada. Si se elimina el último backup protegido, SnapManager pierde la capacidad para identificar las diferencias entre los backups y debe buscar una forma de volver a establecer la base de estas relaciones. Por lo tanto, al intentar eliminar la última copia de seguridad protegida se muestra un mensaje de error.

Solución

Puede eliminar el perfil o sólo la copia de seguridad del perfil.

Para eliminar el perfil, realice los siguientes pasos:

1. Eliminar las copias de seguridad del perfil.
2. Actualice el perfil y desactive la protección en el perfil.

   De esta forma se elimina el conjunto de datos.
3. Elimine la última copia de seguridad protegida.
4. Elimine el perfil.

Para eliminar solamente el backup, realice los siguientes pasos:

1. Cree otra copia de seguridad del perfil.
2. Transferir esa copia de backup a almacenamiento secundario.
3. Elimine la copia de seguridad anterior.

No se pueden gestionar los nombres de destino de los archivos de registro de archivos si los nombres de destino forman parte de otros nombres de destino

Al crear una copia de seguridad del registro de archivos, si el usuario excluye un destino que forme parte de otros nombres de destino, también se excluirán los demás nombres de destino.

Por ejemplo, supongamos que hay tres destinos disponibles para ser excluidos: /Dest, /dest1 y /dest2. Al crear el backup del archivo de registro de archivos, si excluye /dest mediante el comando

```
smo backup create -profile almsamp1 -data -online -archivelogs  -exclude
-dest /dest
```

, SnapManager para Oracle excluye todos los destinos que comiencen con /dest.

Solución

- Agregue un separador de ruta después de que los destinos estén configurados en v$archive_dest. Por ejemplo, cambie /dest a /dest/.
- Al crear una copia de seguridad, incluya destinos en lugar de excluir cualquier destino.

La restauración de archivos de control multiplexados en Automatic Storage Management (ASM) y almacenamiento no ASM falla

Cuando los archivos de control se multiplexan en almacenamiento ASM y no ASM, la operación de copia de seguridad se realiza correctamente. Sin embargo, cuando intenta restaurar archivos de control de ese backup exitoso, se produce un error en la operación de restauración.

Error en la operación de clonado de SnapManager

Al clonar un backup en SnapManager, es posible que DataFabric Manager Server no detecte volúmenes y muestre el siguiente mensaje de error:

SMO-13032: No se puede realizar la operación: Clone Create. Causa raíz: SMO-11007: Error al clonar desde la instantánea: FLOW-11019: Error al 00018 detectar el almacenamiento para /mnt/DataFile_clon3: SD-10016: Error al ejecutar el comando SnapDrive "/usr/sbin/snapdrive Storage show -fs /mnt/DataFile_clon3": 0002-719 Advertencia: No se pudo comprobar el acceso a 20091122235002515 los servidores de almacenamiento de oracle.x.vol1_vol

Motivo: El recurso especificado no es válido. No se puede encontrar su ID en el servidor de Operations Manager 10.x.x.x.

Esto sucede si el sistema de almacenamiento tiene un gran número de volúmenes.

Solución

Debe realizar una de las siguientes acciones:

- Desde el servidor de Data Fabric Manager, ejecute el host dfm Discover Storage_System.

  También puede añadir el comando en un archivo de script del shell y programar una tarea en DataFabric Manager Server para ejecutar el script a intervalos frecuentes.

- Aumente el valor de dfm-rbac-retries en el archivo SnapDrive.conf.

  SnapDrive usa el valor del intervalo de actualización predeterminado y la cantidad predeterminada de reintentos. El valor predeterminado de dfm-rbac-retry-sleep-secs es 15 segundos y dfm-rbac-retries es 12 iteraciones.

  > El intervalo de actualización de Operations Manager depende del número de sistemas de almacenamiento, del número de objetos de almacenamiento del sistema de almacenamiento y de la carga sobre DataFabric Manager Server.

Como recomendación, lleve a cabo lo siguiente:

a. En DataFabric Manager Server, ejecute manualmente el siguiente comando para todos los sistemas de almacenamiento secundarios asociados con el conjunto de datos: El host dfm Discover Storage_system
b. Se debe doble el tiempo que se tarda en ejecutar la operación de detección del host y asignar ese valor a dfm-rbac-retry-sleep-secs.

   Por ejemplo, si la operación tardó 11 segundos, puede establecer el valor de dfm-rbac-retry-sleep-secs en 22 (11*2).

El tamaño de la base de datos del repositorio crece con el tiempo y no con el número de backups

El tamaño de la base de datos del repositorio crece con el tiempo debido a que las operaciones SnapManager insertan o eliminan datos dentro del esquema en las tablas de la base de datos del repositorio, lo que da como resultado un uso elevado del espacio de índice.

Solución

Debe supervisar y reconstruir los índices de acuerdo con las directrices de Oracle para controlar el espacio consumido por el esquema del repositorio.

No se puede acceder a la interfaz gráfica de usuario de SnapManager y se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva

Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

En la siguiente tabla, se enumeran las diferentes acciones que se pueden realizar y sus excepciones:

Operaciones	Excepciones
Abrir un repositorio cerrado	El siguiente mensaje de error se registra en sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: Closed Connection java.sql.SQLException: Closed Connection.
Para actualizar un repositorio abierto, pulse F5	Se muestra una excepción de repositorio en la GUI y también registra una NullPointerException en el archivo sm_gui.log.
Actualizar el servidor host	Se registra una NullPointerException en el archivo sumo_gui.logl.
Creación de un nuevo perfil	Aparecerá NullPointerException en la ventana Profile Configuration.
Actualizar un perfil	La siguiente excepción SQL se registra en sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: Closed Connection.

Obtener acceso a un backup	El siguiente mensaje de error se registra en sm_gui.log: No se pudo inicializar de forma lazilada una colección.
Ver las propiedades de clon	El siguiente mensaje de error se registra en sm_gui.log y sumo_gui.log: No se pudo inicializar de forma lazilada una colección.

Solución

Debe asegurarse de que se ejecute la base de datos del repositorio cuando se desea acceder a la interfaz gráfica de usuario o realizar cualquier operación de SnapManager.

No se pueden crear los archivos temporales para la base de datos clonada

Cuando los archivos de espacio de tabla temporales de la base de datos de destino se colocan en puntos de montaje diferentes del punto de montaje de los archivos de datos, la operación de creación de clonado se realiza correctamente, pero SnapManager no puede crear archivos temporales para la base de datos clonada.

Solución

Debe realizar una de las siguientes acciones:

- Asegúrese de que la base de datos de destino esté diseñada para que los archivos temporales se coloquen en el mismo punto de montaje que los archivos de datos.
- Crear manualmente o añadir archivos temporales en la base de datos clonada.

No se puede migrar el protocolo de NFSv3 a NFSv4

Puede migrar el protocolo de NFSv3 a NFSv4 mediante la habilitación del parámetro enable-migrate-nfs-version en el archivo snapdrive.conf. Durante la migración, SnapDrive considera únicamente la versión del protocolo, independientemente de las opciones de punto de montaje como rw, largefiles, nosuid, etc.

Sin embargo, después de migrar el protocolo a NFSv4, cuando restaura el backup creado mediante NFSv3, se produce lo siguiente:

- Si se habilitan NFSv3 y NFSv4 en el nivel de almacenamiento, la operación de restauración se realiza correctamente, pero se monta con las opciones de punto de montaje que estaban disponibles durante el backup.
- Si solo se habilita NFSv4 en el nivel de almacenamiento, la operación de restauración se realiza correctamente y solo se conserva la versión del protocolo (NFSv4).

  Sin embargo, no se conservan las demás opciones de punto de montaje, como rw, largefiles, nosuid, etc.

Solución

Primero debe apagar manualmente la base de datos, desmontar los puntos de montaje de la base de datos y montarlos con las opciones disponibles antes de la restauración.

Se produce un error en el backup de la base de datos Data Guard en espera

Si se configura alguna ubicación de registro de archivos con el nombre de servicio de la base de datos primaria, se produce un error en el backup de la base de datos en espera de Data Guard.

Solución

En la GUI, debe desactivar **especificar la ubicación del registro de archivo externo** correspondiente al nombre de servicio de la base de datos primaria.

Se produce un error en el montaje de un volumen FlexClone en un entorno NFS

Cuando SnapManager crea un FlexClone de un volumen en un entorno NFS, se añade una entrada en el archivo /etc/exports. El clon o el backup no se pueden montar en un host de SnapManager con un mensaje de error.

El mensaje de error es: 0001-034 error de comando: mount failed: mount: filer1:/vol/SnapManager_20090914112850837_vol14 en /opt/NTAPsmo/mnt/-ora_data02-20090914112850735_1 - WARNING Unknown Option "Zone=vol14" nfs Mount: filer1:/vol/SnapManager_20090914112850837_vol14: Permiso denegado.

Al mismo tiempo, se genera el siguiente mensaje en la consola del sistema de almacenamiento: Mon Sep 14 23:58:37 PDT [filer1: export.auto.update.disabled: warning]: /Etc/exports no se actualizó para vol14 cuando se ejecutó el comando vol clone create. Actualice manualmente /etc/exports o copie /etc/exports.new en él.

Es posible que este mensaje no se capture en los mensajes de AutoSupport.

> Es posible que tenga problemas similares al clonar volúmenes de FlexVol en NFS. Puede seguir los mismos pasos para activar la opción nfs.export.auto-update.

Qué hacer

1. Establezca la opción nfs.export.auto-update activada para que el archivo /etc/exports se actualice automáticamente. opciones nfs.export.auto-updateon

> En la configuración de par de alta disponibilidad, asegúrese de establecer la opción de exportaciones NFS en on para los dos sistemas de almacenamiento.

Se produce un error en la ejecución de varias operaciones paralelas en SnapManager

Cuando se ejecutan varias operaciones en paralelo en bases de datos independientes que residen en el mismo sistema de almacenamiento, el igroup para LUN asociadas con ambas bases de datos puede eliminarse debido a una de las operaciones. Más adelante, si la otra operación intenta utilizar el igroup eliminado, SnapManager muestra un mensaje de error.

Por ejemplo, si ejecuta las operaciones de eliminación de backup y creación de backup en bases de datos diferentes casi al mismo tiempo, la operación de creación de backup generará errores. Los siguientes pasos secuenciales muestran lo que ocurre cuando se ejecutan operaciones de eliminación de backup y creación de backup en distintas bases de datos casi al mismo tiempo.

1. Ejecute el comando backup delete.
2. Ejecute el comando backup create.
3. El comando backup create identifica el igroup ya existente y utiliza el mismo igroup para asignar la LUN.
4. El comando backup delete elimina la LUN de backup, que se asignó al mismo igroup.
5. A continuación, el comando backup delete elimina el igroup porque no hay ninguna LUN asociada con el igroup.
6. El comando backup create crea el backup e intenta asignar al igroup que no existe y, por lo tanto, se produce un error en la operación.

Qué hacer

Debe crear un igroup para cada sistema de almacenamiento utilizado por la base de datos y utilizar el siguiente comando para actualizar SDU con la información del igroup: SnapDrive igroup add

No se puede restaurar la base de datos de RAC desde uno de los nodos de RAC donde no se creó el perfil

En un entorno de Oracle RAC donde ambos nodos pertenecen al mismo clúster, si se intenta realizar una operación de restauración desde un nodo que es diferente del nodo donde se creó el backup, se produce un error en la operación de restauración.

Por ejemplo, si crea un backup en el nodo A e intenta restaurar desde el nodo B, la operación de restauración falla.

Qué hacer

Antes de realizar la operación de restauración desde el nodo B, realice lo siguiente en el nodo B:

1. Añada el repositorio.
2. Sincronice el perfil ejecutando el comando smo profile Sync.
3. Establecer las credenciales del perfil que se utilizará para la operación de restauración ejecutando el comando smo credential set.
4. Actualice el perfil para añadir el nuevo nombre de host y el SID correspondiente ejecutando el comando smo profile update.

Dónde obtener más información

Puede encontrar información sobre las tareas básicas relacionadas con la instalación y el uso de SnapManager.

Documentar	Descripción
Página de descripción de SnapManager	Esta página proporciona información sobre SnapManager, los punteros a la documentación en línea y un enlace a la página de descarga de SnapManager, desde la cual se puede descargar el software.

Documentar	Descripción
Guía de configuración DE SAN Data ONTAP para 7-Mode	Este documento está disponible en "mysupport.netapp.com". Se trata de un documento dinámico online que contiene la información más actualizada sobre los requisitos para configurar un sistema en un entorno SAN. Contiene información detallada sobre sistemas de almacenamiento y plataformas de host, problemas de cableado, problemas de switch y configuraciones.
Matriz de compatibilidad de SnapManager y SnapDrive	Este documento está disponible en la sección interoperabilidad de "mysupport.netapp.com/matrix". Se trata de un documento dinámico online que contiene la información más actualizada específica de SnapManager y sus requisitos de plataforma.
Notas de la versión de SnapManager	Este documento incluye SnapManager. También puede descargar una copia desde "mysupport.netapp.com". Contiene información de última hora que necesita para poner la configuración en funcionamiento sin problemas.
Documentación sobre la conexión para host y los kits de soporte de NetApp	"mysupport.netapp.com".
Guía de configuración del sistema	"mysupport.netapp.com".
Guía de gestión de acceso en bloques de Data ONTAP	"mysupport.netapp.com"
Información del sistema operativo y de la base de datos del host	Estos documentos proporcionan información acerca del sistema operativo del host y el software de la base de datos.

Clasificación de mensajes de error

Puede determinar la causa de un error si conoce las clasificaciones de mensajes.

En la siguiente tabla, se proporciona información acerca de los rangos numéricos de los diferentes tipos de mensajes que puede ver con SnapManager:

Grupo	Rango	Uso
ENTORNO ORACLE	1000-1999	Se utiliza para registrar el estado o los problemas con el entorno operativo de SnapManager. Este grupo incluye mensajes sobre los sistemas con los que SnapManager interactúa, por ejemplo, con el host, el sistema de almacenamiento, la base de datos, etc.
BACKUP	2000-2999	Asociados con el proceso de backup de la base de datos.
RESTAURAR	3000-3999	Asociados con el proceso de restauración de bases de datos.
CLONAR	4000-4999	Asociados con el proceso de clonado de base de datos.
PERFIL	5000-5999	Se utiliza para administrar perfiles.
GESTIONE	6000-6999	Se utiliza para gestionar backups.
INTERFAZ DE BASES DE DATOS VIRTUALES	7000-7999	Asociado con la interfaz de base de datos virtual.
INTERFAZ DE ALMACENAMIENTO VIRTUAL	8000-8999	Asociado con la interfaz de almacenamiento virtual.
REPOSITORIO	9000-9999	Asociado con la interfaz del repositorio.
MÉTRICAS	10000-10999	Asociados con el tamaño del backup de base de datos, tiempo transcurrido para realizar el backup, tiempo para restaurar la base de datos, número de veces que se clona una base de datos, etc.
INTERFAZ DE HOST VIRTUAL	11000-11999	Asociado con la interfaz del host virtual. Esta es la interfaz para el sistema operativo del host.

Grupo	Rango	Uso
EJECUCIÓN	12000-12999	Asociado al paquete de ejecución, incluidas las llamadas al sistema operativo de desove y procesamiento.
PROCESO	13000-13999	Asociado con el componente de proceso de SnapManager.
SERVICIOS PÚBLICOS	14000-14999	Asociados con las utilidades de SnapManager, el contexto global, etc.
VOLCADO/DIAGNÓSTICO	15000-15999	Asociados con operaciones de volcado o diagnóstico.
AYUDA	16000-16999	Asociado con ayuda.
SERVIDOR	17000-17999	Se utiliza en la administración del servidor SnapManager.
API	18000-18999	Asociado con la API.
AUTOR	20000-20999	Asociado con la autorización de credenciales.

Mensajes de error

Es posible encontrar información sobre los mensajes de error asociados a diferentes operaciones de SnapManager.

Mensajes de error más comunes

En la siguiente tabla se enumeran algunos de los errores más comunes e importantes asociados con SnapManager para Oracle:

Mensaje de error	Explicación	Resolución
SD-10038: El sistema de archivos no se puede escribir.	El proceso de SnapManager no tiene acceso de escritura al sistema de archivos.	Debe asegurarse de que el proceso de SnapManager tenga acceso de escritura al sistema de archivos. Después de corregir esto, es posible que deba tomar otra instantánea.

Mensaje de error	Explicación	Resolución
SMO-05075: No se puede crear el perfil. Debe configurar la relación DP/XDP correctamente o elegir la política de protección correcta según la relación subyacente.	Los volúmenes subyacentes no están en una relación de SnapVault ni de SnapMirror.	Debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.
SMO-05503: Se ha especificado el mismo nombre al perfil. Especifique un nombre diferente para cambiar el nombre del perfil.	Los perfiles con nombres idénticos no pueden existir en un repositorio.	Introduzca un nombre de perfil que no esté en uso.
SMO-05505: No se pueden actualizar los metadatos del conjunto de datos.	Es posible que el conjunto de datos se haya eliminado o no exista.	Antes de actualizar los metadatos del conjunto de datos, compruebe que el conjunto de datos existe mediante la consola de gestión de NetApp.
SMO-05506: No se puede actualizar el perfil porque hay operaciones en ejecución en el perfil. Debe esperar hasta que la operación o operaciones se completen y, a continuación, actualizar el perfil.	El perfil no se puede actualizar cuando hay operaciones de backup, restauración y clonado en curso.	Actualice el perfil una vez completada la operación actual.
SMO-05509: Duración de la retención primaria de archive velog no válida; especifique un valor entero positivo.	La duración de la retención de los backups de registros de archivos no puede ser negativa.	Especifique un valor positivo para la duración de la retención de los backups de registros de archivos.
SMO-07463: Esta restauración de backups requiere que la base de datos esté en el estado requerido. Error al llevar la base de datos al estado requerido.	La base de datos no está en el estado requerido para una operación de backup.	Compruebe que la base de datos esté en estado relevante antes de crear una copia de backup. El estado de la base de datos que se va a restaurar depende del tipo de proceso de restauración que se desee realizar y del tipo de archivos que se incluirán.
SMO-09315: Después de realizar una actualización o una operación de actualización del repositorio, es posible que no se reciba la notificación de resumen para las notificaciones establecidas en la versión anterior, a menos que se actualice la notificación de resumen con los detalles del host de notificación.	Los ajustes de notificación no se configuran para el repositorio después de una actualización gradual.	Después de una actualización gradual, actualice la configuración de notificación de resumen para recibir notificaciones.

Mensaje de error	Explicación	Resolución
SM0-02076: El nombre de la etiqueta no debe contener ningún carácter especial que no sea el guión bajo.	El nombre de la etiqueta contiene caracteres especiales distintos del guión bajo.	El nombre de la etiqueta debe ser único dentro del perfil. El nombre puede contener letras, números, un guión bajo (_) y un guión (-) (pero no puede comenzar con un guión). Asegúrese de que las etiquetas no contengan caracteres especiales excepto el guion bajo.
SMO-06308: Excepción al intentar iniciar la programación: java.lang.NullPointerException	Se configura el nombre de dominio completo (FQDN) del host de perfil en lugar del nombre de host del sistema y no se puede resolver el FQDN del host de perfil.	Asegúrese de usar el nombre de host del sistema y no el FQDN.
Error en ExecuteRestoreSteps: ORACLE-10003: Error al ejecutar SQL "DROP DISKGROUP;control nombre del grupo de discos; INCLUIDO CONTENIDO" contra la base de datos Oracle +ASM1: ORA-15039: diskgroup no eliminados ORA-15027: Uso activo del grupo de discos; "control del nombre del grupo de discos;" impide su desmontaje	La operación para restaurar un backup con archivos de control no puede soltar el grupo de discos de control. Este problema ocurre si hay archivos de control de copia de seguridad obsoletos en el grupo de discos de control.	Identifique los archivos de control de copia de seguridad obsoletos y elimínelos manualmente.
RMAN-06004: Error DE ORACLE de la base de datos del catálogo de recuperación: ORA-01424: Carácter ausente o ilegal después del carácter de escape	La operación de creación de backup no se pudo quitar la copia de backup del catálogo cuando SnapManager está integrada con RMAN.	Compruebe si hay secuencias de comandos externas utilizadas para eliminar las copias de seguridad de RMAN. Ejecute el comando CROSSCHECK BACKUP en RMAN para actualizar el repositorio de RMAN y el comando resync catalog para sincronizar el archivo de control de la base de datos de destino con el catálogo de recuperación.
[DEBUG]: Excepción al eliminar la copia de seguridad. java.lang.IllegalStateException: [Assertion failed] - este estado invariante debe ser true	Se crean múltiples copias de Snapshot para un solo ID de operación.	Eliminar las copias Snapshot manualmente y utilizar scripts para eliminar las entradas del repositorio.
La hora y la hora del sistema que muestra SnapManager en los archivos de registro no coinciden o no están sincronizados.	Java 7 aún no admite un cambio de zona horaria.	Aplique la revisión tzUpdater proporcionada por Oracle.

Mensaje de error	Explicación	Resolución
DISC-00001: No se puede detectar almacenamiento: El siguiente identificador no existe o no es del tipo esperado: Archivo ASM	Los archivos de datos o de control o los redo logs se multiplexan en una base de datos ASM.	Extraiga el multiplexado de Oracle.
ORA-01031: Privilegios insuficientes. Compruebe que el servicio Windows de SnapManager está configurado para ejecutarse como usuario con los privilegios correctos y que el usuario está incluido en el grupo ORA_DBA.	No tiene privilegios suficientes en SnapManager. La cuenta de servicio de SnapManager no forma parte del grupo ORA_DBA.	Haga clic con el botón derecho del ratón en el icono **PC** del escritorio y seleccione **gestionar** para comprobar que la cuenta de usuario del servicio SnapManager forma parte del grupo ORA_DBA. Compruebe los usuarios y grupos locales y asegúrese de que la cuenta forma parte del grupo ORA_DBA. Si el usuario es el administrador local, asegúrese de que el usuario está en el grupo en lugar del administrador del dominio.
0001-CON-10002: Los discos ASM conectados con rutas <paths> no fueron detectados por la instancia de ASM <asm_instance_sid>. Verifique que el parámetro ASM_DISKSTRING y los permisos del sistema de archivos permiten detectar estas rutas.	Los discos ASM se conectaron al host, pero la instancia de ASM no puede detectarlos.	Si se está utilizando ASM sobre NFS, asegúrese de que el parámetro ASM_DISKSTRING para la instancia de ASM incluye los archivos de disco de ASM. Por ejemplo, si el error indica: smo/mnt/<dir_name>/<disk_name> , agregue /smo/mnt/**/** a asm_diskstring.
0001-DS-10021: No se puede establecer la política de protección del conjunto de datos <dataset-name> en <new-protection-policy> porque la política de protección ya está configurada en <old-protection-policy>. Utilice Protection Manager para cambiar la política de protección	Una vez establecida la política de protección de un conjunto de datos, SnapManager no le permitirá cambiar la política de protección, ya que puede requerir volver a alinear las relaciones de base y provocar la pérdida de backups existentes en el almacenamiento secundario.	Actualice la política de protección mediante la consola de gestión de Protection Manager, que proporciona más opciones para migrar de una política de protección a otra.
0001-SD-10028: Error SnapDrive (id:2618 code:102) no se puede detectar el dispositivo asociado a "lun_path". Si se utiliza la multivía, es posible que se produzca un error de configuración de multivía. Verifique la configuración e inténtelo de nuevo.	El host no puede detectar las LUN creadas en los sistemas de almacenamiento.	Asegúrese de que el protocolo de transporte está correctamente instalado y configurado. Asegúrese de que SnapDrive pueda crear y detectar una LUN en el sistema de almacenamiento.

Mensaje de error	Explicación	Resolución
0001-SD-10028: Error de SnapDrive (ID:2836 código:110) error al adquirir el bloqueo del conjunto de datos en el volumen "Storage name":"temp_volume_name"	Se intentó restaurar con el método de almacenamiento indirecto y el volumen temporal especificado no existe en el almacenamiento primario.	Cree un volumen temporal en el almacenamiento primario. O bien, especifique el nombre correcto del volumen si ya se ha creado un volumen temporal.
0001-SMO-02016: Es posible que haya habido tablas externas en la base de datos de las que no se ha realizado un backup como parte de esta operación de backup (ya que la base de datos no estaba ABIERTA durante esta copia de seguridad ALL_EXTERNAL_LOCATIONS no se pudo consultar para determinar si existen tablas externas o no).	SnapManager no realiza copias de seguridad de tablas externas (por ejemplo, tablas que no están almacenadas en archivos .dbf). Este problema se produce porque la base de datos no estaba abierta durante el backup, SnapManager no puede determinar si se están utilizando tablas externas.	Puede haber tablas externas en la base de datos que no se incluyeron en un backup como parte de esta operación (porque la base de datos no estaba abierta durante el backup).
0001-SMO-11027: No se pueden clonar o montar snapshots desde el almacenamiento secundario porque las snapshots están ocupadas. Intente clonar o montar a partir de un backup más antiguo.	Intentó crear una clonación o montar copias Snapshot a partir del almacenamiento secundario del backup protegido más reciente.	Clone o monte desde un backup anterior.
0001-SMO-12346: No se pueden enumerar las políticas de protección porque el producto Protection Manager no está instalado o SnapDrive no está configurado para utilizarlo. Instale Protection Manager y/o configure SnapDrive…	Se intentó enumerar las políticas de protección en un sistema donde SnapDrive no se configuró para usar Protection Manager.	Instale Protection Manager y configure SnapDrive para que use Protection Manager.
0001-SMO-13032: No se puede realizar la operación: Eliminación de backups. Causa raíz: 0001-SMO-02039: No se puede eliminar el backup del conjunto de datos: SD-10028: Error de SnapDrive (id:2406 código:102) no se pudo eliminar el ID de backup: "Backup_id" para el conjunto de datos, error(23410):Snapshot "snapshot_name" en el volumen "volume_name" está ocupado.	Intentó liberar o eliminar el backup protegido más reciente o un backup que contiene copias de Snapshot que son bases de referencia en una relación de mirroring.	Libere o elimine el backup protegido.

Mensaje de error	Explicación	Resolución
0002-332 error de administrador: No se ha podido comprobar SD.snapshot.Clone el acceso al volumen "volume_name" del nombre de usuario de usuario en los servidores de Operations Manager "dfm_Server". Motivo: El recurso especificado no es válido. No se puede encontrar su ID en Operations Manager Server "dfm_Server"	No se han configurado los privilegios de acceso adecuados y los roles.	Defina los privilegios de acceso o los roles para los usuarios que intentan ejecutar el comando.
[WARN] FLOW-11011: Operación cancelada [ERROR] FLOW-11008: Error de operación: Error de operación: Espacio de pila Java.	Hay más archivos de registro de archivos en la base de datos que el máximo permitido.	1. Desplácese hasta el directorio de instalación de SnapManager. 2. Abra el archivo Launch-java. 3. Aumente el valor de `java -Xmx160m` Parámetro Java heap space . Por ejemplo, puede modificar el valor del valor predeterminado de 160 m a 200 m. `java -Xmx200m`.
SD-10028: Error de SnapDrive (id:2868 code:102) no se pudo encontrar la instantánea remota ni el qtree remoto.	SnapManager muestra los backups como protegidos aunque el trabajo de protección de Protection Manager solo se haya realizado correctamente parcialmente. Esta condición ocurre cuando la conformidad del conjunto de datos está en curso (cuando las Snapshot básicas se están reflejando).	Realizar un nuevo backup tras el conjunto de datos conforme a las exigencias.
SMO-21019: No se pudo realizar la poda del registro de archivo para el destino: "/mnt/destination_name/" con el motivo: "ORACLE-00101: Error al ejecutar el comando de RMAN: [DELETE NOPROMET ARCHIVELOG '/mnt/destination_name/']	La eliminación del registro de archivo falla en uno de los destinos. En este caso, SnapManager continúa depurando los archivos de registro de archivos de los otros destinos. Si algún archivo se elimina manualmente del sistema de archivos activo, RMAN no puede hacer una copia de los archivos de registro de archivos de ese destino.	Conéctese a RMAN desde el host SnapManager. Ejecute el comando CROSSCHECK ARCHIVELOG ALL de RMAN y vuelva a realizar la operación de eliminación en los archivos de registro de archivos.

Mensaje de error	Explicación	Resolución
SMO-13032: No se puede realizar la operación: Archive log Prune. Causa raíz: Excepción de RMAN: ORACLE-00101: Error al ejecutar el comando RMAN.	Los archivos de registro de archivos se eliminan manualmente de los destinos de registro de archivos.	Conéctese a RMAN desde el host SnapManager. Ejecute el comando CROSSCHECK ARCHIVELOG ALL de RMAN y vuelva a realizar la operación de eliminación en los archivos de registro de archivos.
No se puede analizar la salida del shell: (java.util.regex.Matcher[pattern=Command Complete. Region=0,18 lastmatch=]) no coincide (name:backup_script) no se puede analizar la salida del shell: (java.util.regex.Matcher[pattern=Command complete. region=0,25 lastmatch=]) no coincide (description:script backup) No se puede analizar la salida del shell: (java.util.regex.Matcher[pattern=Command Complete. region=0,9 lastmatch=]) no coincide (timeout:0)	Las variables de entorno no se definen correctamente en los scripts previos o posteriores a las tareas.	Compruebe si las secuencias de comandos previas o posteriores a las tareas siguen la estructura del complemento SnapManager estándar. Para obtener información adicional sobre el uso de las variables de entorno en el script, consulte Operaciones en scripts de tareas.
ORA-01450: Se ha superado la longitud máxima de la llave (6398).	Cuando se realiza una actualización de SnapManager 3.2 para Oracle a SnapManager 3.3 para Oracle, la operación de actualización se produce un error con este mensaje de error. Este problema puede ocurrir debido a uno de los siguientes motivos: • El tamaño de bloque del tablespace en el que existe el repositorio es inferior a 8k. • El parámetro nls_length_semántica se establece en char.	Debe asignar los valores a los siguientes parámetros: • block_size=8192 • nls_length=byte Después de modificar los valores de los parámetros, debe reiniciar la base de datos. Para obtener más información, consulte el artículo 2017632 de la base de conocimientos.

Mensajes de error asociados con el proceso de copia de seguridad de la base de datos (serie 2000)

En la siguiente tabla se enumeran los errores comunes asociados al proceso de copia de seguridad de la base de datos:

Mensaje de error	Explicación	Resolución

SMO-02066: No es posible eliminar ni liberar los "registros de datos" del backup de registros de archivo, ya que el backup está asociado a los "registros de datos" del backup de datos.	La copia de seguridad del registro de archivos se realiza junto con la copia de seguridad de los archivos de datos y se intentó eliminar el backup del registro de archivos.	Utilice la opción -force para eliminar o liberar el backup.
SMO-02067: No se puede eliminar ni liberar los "registros de datos" del backup de registros de archivo, ya que el backup está asociado a los "registros de datos" del backup de datos y se encuentra dentro de la duración de retención asignada.	El backup de registros de archivos se asocia con el backup de la base de datos y se encuentra dentro del período de retención, y se intentó eliminar el backup de registros de archivos.	Utilice la opción -force para eliminar o liberar el backup.
SMO-07142: Registros archivados excluidos debido al patrón de exclusión <exclusion>.	Se excluyen algunos archivos de registro de archivos durante la operación de creación de perfiles o creación de copias de seguridad.	No se requiere ninguna acción.
SMO-07155: Los archivos de registro archivados de <count> no existen en el sistema de archivos activo. Estos archivos de registro archivados no se incluirán en la copia de seguridad.	Los archivos de registro de archivos no existen en el sistema de archivos activo durante la operación de creación de perfiles o de creación de backup. Estos archivos de registro archivados no se incluyen en la copia de seguridad.	No se requiere ninguna acción.
SMO-07148: Los archivos de registro archivados no están disponibles.	No se crean archivos de registro de archivos para la base de datos actual durante la operación de creación de perfiles o creación de backups.	No se requiere ninguna acción.
SMO-07150: No se encuentran los archivos de registro archivados.	Faltan todos los archivos de registro de archivos del sistema de archivos o se excluyen durante la operación de creación de perfiles o creación de copia de seguridad.	No se requiere ninguna acción.

SMO-13032: No se puede realizar la operación: Crear un backup. Causa raíz: ORACLE-20001: Error al intentar cambiar el estado A ABIERTO para la instancia de base de datos dfcln1: ORACLE-20004: Esperando poder abrir la base de datos sin la opción RESETLOGS, pero oracle está informando de que la base de datos necesita abrirse con la opción RESETLOGS. Para evitar que se restableciendo inesperadamente los registros, el proceso no continuará. Asegúrese de que la base de datos se puede abrir sin la opción RESETLOGS e inténtelo de nuevo.	Se intenta realizar una copia de seguridad de la base de datos clonada que se creó con la opción -no-resetlogs. La base de datos clonada no es una base de datos completa. Sin embargo, es posible realizar operaciones de SnapManager, como crear perfiles y backups, dividir clones, etc. con la base de datos clonada, pero se produce un error en las operaciones de SnapManager debido a que la base de datos clonada no se configura como una base de datos completa.	Recuperar la base de datos clonada o convertir la base de datos a una base de datos de Data Guard en espera.

Errores de protección de datos

En la siguiente tabla se muestran los errores comunes asociados con la protección de datos:

Mensaje de error	Explicación	Resolución
Se solicita la protección de backup, pero el perfil de base de datos no tiene una política de protección. Actualice la política de protección en el perfil de la base de datos o no utilice la opción "proteger" al crear backups.	Se intenta crear un backup con protección en el almacenamiento secundario; sin embargo, el perfil asociado a este backup no tiene una política de protección especificada.	Edite el perfil y seleccione una política de protección. Vuelva a crear el backup.
No se puede eliminar el perfil porque la protección de datos está habilitada, pero Protection Manager no está disponible temporalmente. Inténtelo de nuevo más tarde, por favor.	Se intenta eliminar un perfil que tiene la protección habilitada; sin embargo, Protection Manager no está disponible.	Asegúrese de que los backups adecuados se almacenen en el almacenamiento primario o secundario. Desactive la protección en el perfil. Cuando Protection Manager esté disponible de nuevo, vuelva al perfil y elimínelo.
No se puede enumerar las políticas de protección porque Protection Manager no está disponible temporalmente. Inténtelo de nuevo más tarde, por favor.	Al configurar el perfil de backup, debe habilitar la protección en el backup para que el backup se almacene en el almacenamiento secundario. Sin embargo, SnapManager no puede recuperar las políticas de protección de la consola de gestión de Protection Manager.	Desactive la protección en el perfil temporalmente. Continúe creando un nuevo perfil o actualizando un perfil existente. Cuando Protection Manager esté disponible de nuevo, vuelva al perfil.

No se pueden enumerar las políticas de protección porque el producto Protection Manager no está instalado o SnapDrive no está configurado para utilizarlo. Instale Protection Manager o configure SnapDrive.	Al configurar el perfil de backup, debe habilitar la protección en el backup para que el backup se almacene en el almacenamiento secundario. Sin embargo, SnapManager no puede recuperar las políticas de protección de la Consola de gestión de Protection Manager. Protection Manager no está instalado o SnapDrive no está configurado.	Instale Protection Manager. Configure SnapDrive. Vuelva al perfil, vuelva a activar la protección y seleccione las políticas de protección disponibles en la consola de gestión de Protection Manager.
No se puede establecer la política de protección porque Protection Manager no está disponible temporalmente. Inténtelo de nuevo más tarde, por favor.	Al configurar el perfil de backup, debe habilitar la protección en el backup para que el backup se almacene en el almacenamiento secundario. Sin embargo, SnapManager no puede recuperar las políticas de protección de la Consola de gestión de Protection Manager.	Desactive la protección en el perfil temporalmente. Continúe creando o actualizando el perfil. Cuando la Consola de administración de Protection Manager esté disponible, vuelva al perfil.
Creación de un nuevo conjunto de datos <dataset_name> para base de datos <dbname> en la <host> del host.	Ha intentado crear un perfil de copia de seguridad. SnapManager crea un conjunto de datos para este perfil.	No es necesario realizar ninguna acción.
La protección de datos no está disponible porque Protection Manager no está instalado.	Al configurar el perfil de backup, se intentó habilitar la protección en el backup para que el backup se almacenara en el almacenamiento secundario. Sin embargo, SnapManager no puede acceder a las políticas de protección desde la consola de gestión de Protection Manager. Protection Manager no está instalado.	Instale Protection Manager.
Se ha eliminado el <dataset_name> de conjunto de datos para esta base de datos.	Ha eliminado un perfil. SnapManager eliminará el conjunto de datos asociado.	No es necesario realizar ninguna acción.
La eliminación de perfiles con protección habilitada y Protection Manager ya no está configurada. Eliminar perfil de SnapManager pero no limpiar conjunto de datos en Protection Manager.	Se intentó eliminar un perfil que tiene la protección habilitada; sin embargo, Protection Manager ya no está instalado o ya no está configurado o ha caducado. SnapManager eliminará el perfil, pero no el conjunto de datos del perfil de la consola de gestión de Protection Manager.	Vuelva a instalar o vuelva a configurar Protection Manager. Vuelva al perfil y elimínelo.

Clase de retención no válida. Use el término «ayuda de smo» para ver una lista de las clases de retención disponibles.	Al configurar la directiva de retención, intentó utilizar una clase de retención no válida.	Crear una lista de clases de retención válidas introduciendo este comando: SMO ayuda a backup Actualice la directiva de retención con una de las clases disponibles.
La política de protección especificada no está disponible. Use «lista de normativas de protección de smo» para ver una lista de las normativas de protección disponibles.	Al configurar el perfil, debe habilitar la protección e introducir una política de protección que no esté disponible.	Identifique las políticas de protección disponibles introduciendo el siguiente comando: Lista de políticas de protección de smo
Utilizar el conjunto de datos existente <dataset_name> para Database <dbname> en el <host> del host, dado que el conjunto de datos ya existía.	Intentó crear un perfil; sin embargo, el conjunto de datos para el mismo perfil de base de datos ya existe.	Compruebe las opciones del perfil existente y asegúrese de que coinciden con lo que necesita en el nuevo perfil.
Utilizar el conjunto de datos existente <dataset_name> para la base de datos RAC <dbname> desde el perfil <profile_name> para la misma base de datos de RAC ya existe, por ejemplo, <SID> en la <hostname> del host.	Intentó crear un perfil para una base de datos RAC; sin embargo, el conjunto de datos para el mismo perfil de base de datos RAC ya existe.	Compruebe las opciones del perfil existente y asegúrese de que coinciden con lo que necesita en el nuevo perfil.
El conjunto de datos <dataset_name> con la política de protección <existing_policy_name> ya existe para esta base de datos. Especificó la política de protección <new_policy_name>. La política de protección del conjunto de datos se modificará a <new_policy_name>. Puede cambiar la política de protección actualizando el perfil.	Ha intentado crear un perfil con la protección activada y una política de protección seleccionada. Sin embargo, el conjunto de datos para el mismo perfil de base de datos ya existe, pero tiene una política de protección diferente. SnapManager usará la política recién especificada para el conjunto de datos existente.	Revise esta política de protección y determine si esta es la política que desea usar para el conjunto de datos. Si no es así, edite el perfil y cambie la directiva.

Protection Manager elimina los backups locales que ha creado SnapManager para Oracle	La consola de gestión de Protection Manager elimina o libera los backups locales creados por SnapManager de acuerdo con la política de retención definida en Protection Manager. La clase de retención establecida para los backups locales no se considera mientras se eliminan o liberan los backups locales.cuando los backups locales se transfieren a un sistema de almacenamiento secundario, no se considera la clase de retención establecida para los backups locales en el sistema de almacenamiento primario. La clase de retención especificada en el programa de transferencia se asigna a la copia de seguridad remota.	Ejecute el comando dfpm Dataset fix_smo desde el servidor Protection Manager cada vez que se crea un nuevo conjunto de datos.ahora los backups no se eliminan de acuerdo con la normativa de retención definida en la consola de gestión de Protection Manager.

Ha seleccionado desactivar la protección para este perfil. Esto podría eliminar potencialmente el conjunto de datos asociado en Protection Manager y destruir las relaciones de replicación creadas para ese conjunto de datos. Tampoco podrá ejecutar operaciones de SnapManager, como restaurar o clonar backups secundarios o terciarios para este perfil. ¿Desea continuar (S/N)?	Intentó deshabilitar la protección para un perfil protegido al actualizar el perfil desde la interfaz gráfica de usuario o la interfaz de línea de comandos de SnapManager. Puede deshabilitar la protección para el perfil mediante la opción -noProtect desde la interfaz de línea de comandos de SnapManager o desactivando la casilla de verificación **Directiva de protección de Protection Manager** en la ventana Propiedades de directivas de la interfaz gráfica de usuario de SnapManager. Cuando se deshabilita la protección para el perfil, SnapManager para Oracle elimina el conjunto de datos de la consola de gestión de Protection Manager, que cancela el registro de todas las copias de backup secundarias y terciarias asociadas con ese conjunto de datos. Tras eliminar un conjunto de datos, todas las copias de backup secundarias y terciarias se huérfanas. Ni Protection Manager ni SnapManager para Oracle tienen la capacidad de acceder a esas copias de backup. Ya no es posible restaurar las copias de backup con SnapManager para Oracle. Se muestra el mismo mensaje de advertencia incluso cuando el perfil no está protegido.	Este es un problema conocido en SnapManager para Oracle y el comportamiento esperado dentro de Protection Manager al destruir un conjunto de datos. No existe ninguna solución alternativa.los backups huérfanos deben gestionarse manualmente.

Mensajes de error asociados con el proceso de restauración (serie 3000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de restauración:

Mensaje de error	Explicación	Resolución

SMO-03031:Restore especifica para restaurar el <variable> de backup, pues los recursos de almacenamiento para el backup ya se han liberado.	Intentó restaurar una copia de seguridad que tiene liberados sus recursos de almacenamiento sin especificar una especificación de restauración.	Especifique una especificación de restauración.
SMO-03032:Restore especificación debe contener asignaciones para los archivos que restaurar, pues los recursos de almacenamiento del backup ya se han liberado. Los archivos que necesitan asignaciones son: <variable> desde instantáneas: <variable>	Intentó restaurar una copia de seguridad que tiene liberados sus recursos de almacenamiento junto con una especificación de restauración que no contiene la asignación de todos los archivos que se van a restaurar.	Corrija el archivo de especificación de restauración de modo que las asignaciones coincidan con los archivos que se van a restaurar.
ORACLE-30028: No se puede volcar el <filename> del archivo de registro. Es posible que el archivo esté ausente/inaccesible/dañado. Este archivo de registro no se utilizará para la recuperación.	Los archivos redo log en línea o los archivos archive log no se pueden utilizar para la recuperación.este error se produce debido a los siguientes motivos: • Los archivos redo log en línea o los archivos archive log mencionados en el mensaje de error no tienen números de cambio suficientes para solicitar la recuperación. Esto ocurre cuando la base de datos está en línea sin ninguna transacción. Los archivos redo log o archive log no tienen ningún número de cambio válido que se pueda aplicar para la recuperación. • El archivo redo log en línea o el archivo archive log mencionado en el mensaje de error no tiene suficientes privilegios de acceso para Oracle. • El archivo redo log en línea o el archivo de registro archivado mencionado en el mensaje de error están dañados y Oracle no puede leerlos. • El archivo redo log en línea o el archivo de registro archivado mencionado en el mensaje de error no se encuentra en la ruta de acceso mencionada.	Si el archivo mencionado en el mensaje de error es un archivo de registro archivado y si ha proporcionado manualmente para la recuperación, asegúrese de que el archivo tiene permisos de acceso completo a Oracle.incluso si el archivo tiene permisos completos, y el mensaje continúa, el archivo de registro de archivo no tiene ningún número de cambio que se aplicará para la recuperación, y este mensaje puede ignorarse.

SMO-03038: No se puede restaurar desde el almacenamiento secundario porque los recursos de almacenamiento siguen existiendo en el volumen primario. Restaure desde el primario.	Intentó restaurar desde el almacenamiento secundario, pero existen copias Snapshot en el almacenamiento primario.	Restaure siempre desde el principal si el backup no se ha liberado.
SM0-03054: Montaje del arco de respaldo para alimentar archivvelogs. DS-10001: Puntos de montaje de conexión. [ERROR] FLOW-11019: Error en ExecuteConnectionSteps: SD-10028: Error de SnapDrive (id:2618 code:305). No se han podido eliminar los siguientes archivos. Es posible que los volúmenes correspondientes sean de solo lectura. Vuelva a intentar el comando con snapshots antiguas.[ERROR] FLOW-11010: Operación que realiza la transición para cancelar debido a un fallo anterior.	Durante la recuperación, SnapManager intenta montar el backup más reciente del sistema secundario para alimentar los archivos de registro de archivos desde el secundario. Sin embargo, si hay otros backups, la recuperación puede tener éxito. Sin embargo, si no hay otros backups, es posible que se produzca un error en la recuperación.	No elimine los backups más recientes del almacenamiento primario, por lo que SnapManager puede utilizar el backup principal para la recuperación.

Mensajes de error asociados con el proceso de clonación (serie 4000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de clonación:

Mensaje de error	Explicación	Resolución
SMO-04133: El destino de volcado no debe existir	Se está utilizando SnapManager para crear nuevos clones; sin embargo, los destinos de volcado que usará el nuevo clon ya existen. SnapManager no puede crear un clon si existen destinos de volcado.	Quite o cambie el nombre de los destinos de volcado antiguos antes de crear un clon.
SMO-04908: No es un FlexClone.	El clon es un clon LUN. Esto se aplica tanto a Data ONTAP 8.1 7-Mode como a Clustered Data ONTAP.	SnapManager admite la división de clones únicamente en la tecnología FlexClone.
SMO-04904: No se ejecuta ninguna operación de división de clones con split-idsplit_id	El ID de la operación no es válido o no hay ninguna operación de división de clones en curso.	Proporcione un ID de división o una etiqueta de división válidos para el estado de división de clones, resultados y operaciones de detención.

SMO-04906: Se ha producido un error en la operación de detención de división de clones con split_id	Se ha completado la operación de división.	Compruebe si el proceso de división en curso mediante el comando clone split-status o clone split-result.
SMO-13032: No se puede realizar la operación: Clone Create. Causa raíz: ORACLE-00001: Error al ejecutar SQL: [ALTER DATABASE OPEN RESETLOGS;]. El comando devolvió: ORA-38856: No se puede marcar la instancia UNNAMED_INSTANCE_2 (redo thread 2) como habilitada.	Se produce un error en la creación del clon cuando se crea desde la base de datos en espera con la siguiente configuración: • La base de datos primaria es una configuración de RAC y la base de datos en espera es independiente. • El modo de espera se crea mediante RMAN para realizar una copia de seguridad de los archivos de datos.	Añada el parámetro _no_recovery_through_resetlogs= TRUE en el archivo de especificación del clon antes de crearlo. Consulte la documentación de Oracle (ID 334899.1) para obtener información adicional. Asegúrese de tener el nombre de usuario y la contraseña de Oracle metalink.
	No ha especificado un valor para un parámetro en el archivo de especificación del clon.	Debe proporcionar un valor para el parámetro o eliminar ese parámetro si no es necesario en el archivo de especificación del clon.

Mensajes de error asociados con el proceso de gestión de perfiles (serie 5000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de clonación:

Mensaje de error	Explicación	Resolución
SMO-20600: No se ha encontrado el perfil "profile1" en el repositorio "repo_name". Ejecute "Profile SYNC" para actualizar las asignaciones de perfil a repositorio.	La operación de volcado no se puede realizar cuando se produce un error al crear el perfil.	Utilice el sistema de volcado.

Mensajes de error asociados con la liberación de recursos de backup (series de backups 6000)

En la siguiente tabla se muestran los errores comunes asociados con las tareas de backup:

Mensaje de error	Explicación	Resolución
SMO-06030: No se puede eliminar el backup porque está en uso: <variable>	Se intentó realizar la operación de backup libre con comandos, cuando el backup está montado o tiene clones, o bien se Marca para que se conserve de forma ilimitada.	Desmonte el backup o cambie la política de retención ilimitada. Si hay clones, elimínelos.

SMO-06045: No se puede liberar el <variable> de backup porque los recursos de almacenamiento para el backup ya se han liberado	Se intentó realizar la operación de backup libre con comandos, cuando ya se ha liberado el backup.	No se puede liberar la copia de seguridad si ya se ha liberado.
SMO-06047: Solo se pueden liberar los backups realizados correctamente. El estado de <ID> de backup es <status>.	Se intentó realizar la operación de backup libre con comandos, cuando el estado del backup no es correcto.	Vuelva a intentarlo después de realizar el backup correctamente.
SMO-13082: No es posible realizar una operación de <variable> en la <ID> de backup porque se han liberado los recursos de almacenamiento para el backup.	Con comandos, se intentó montar un backup con los recursos de almacenamiento liberados.	No es posible montar, clonar o verificar un backup que tenga liberados sus recursos de almacenamiento.

Errores de interfaz de almacenamiento virtual (serie 8000 de interfaz de almacenamiento virtual)

La siguiente tabla muestra los errores comunes asociados con las tareas de interfaz de almacenamiento virtual:

Mensaje de error	Explicación	Resolución
Error de SMO-08017 al detectar almacenamiento para /.	SnapManager intentó localizar recursos de almacenamiento pero encontró archivos de datos, archivos de control o registros en el directorio raíz/. Estos archivos deben residir en un subdirectorio. El sistema de archivos raíz puede ser un disco duro en su equipo local. SnapDrive no puede hacer copias snapshot en esta ubicación y SnapManager no puede realizar operaciones con estos archivos.	Compruebe si los archivos de datos, los archivos de control o los registros de recuperación están en el directorio raíz. Si es así, muévalos a sus ubicaciones correctas o vuelva a crear archivos de control o redo logs en sus ubicaciones correctas. Por ejemplo: Mueva redo.log a /data/oracle/redo.log, donde /data/oracle es el punto de montaje.

Mensajes de error asociados con el proceso de actualización gradual (serie 9000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de actualización gradual:

Mensaje de error	Explicación	Resolución
SMO-09234: Los hosts siguientes no existen en el almacén antiguo. <hostnames>.	Intentó realizar una actualización gradual de un host, que no existe en la versión de repositorio anterior.	Compruebe si el host existe en el repositorio anterior con el comando Repository show-Repository de la versión anterior de la interfaz de línea de comandos de SnapManager.

SMO-09255: Los hosts siguientes no existen en el nuevo almacén. <hostnames>.	Intentó realizar la reversión de un host, que no existe en la versión del nuevo repositorio.	Compruebe si el host existe en el nuevo repositorio con el comando Repository show-Repository de la versión posterior de la CLI de SnapManager.
SMO-09256:Rollback no se admite, ya que existe un nuevo perfil <profilenames>.for the hosts <hostnames> especificados.	Intentó revertir un host que contiene nuevos perfiles existentes en el repositorio. Sin embargo, estos perfiles no existían en el host de la versión anterior de SnapManager.	Elimine nuevos perfiles en la versión posterior o actualizada de SnapManager antes de la reversión.
SMO-09257:Rollback no se admite, ya que los backups <backupid> están montados en los nuevos hosts.	Intentó revertir una versión posterior del host SnapManager que tiene backups montados. Estos backups no se montan en la versión anterior del host SnapManager.	Desmonte los backups en la versión posterior del host SnapManager y, a continuación, realice la reversión.
SMO-09258: No se admite la reversión, ya que los backups <backupid> se desasocian de los nuevos hosts.	Ha intentado revertir una versión posterior del host SnapManager que tiene backups que se están desdesmontan.	Monte los backups en la versión posterior del host SnapManager y, a continuación, ejecute la reversión.
SMO-09298: No se puede actualizar este almacén porque ya tiene otros hosts en la versión superior. En su lugar, ejecute rollingupgrade para todos los hosts.	Realizó una actualización gradual en un solo host y, después, actualizó el repositorio para ese host.	Realice una actualización gradual en todos los hosts.
SMO-09297: Se ha producido un error al habilitar las restricciones. El repositorio puede estar en estado incoherente. Se recomienda restaurar el backup del repositorio que haya tomado antes de la operación actual.	Se intentó realizar una operación de reversión o actualización sucesiva si la base de datos del repositorio queda en estado incoherente.	Restaurar el repositorio del que se ha hecho backup anteriormente.

Ejecución de operaciones (serie 12,000)

En la siguiente tabla se muestran los errores comunes asociados a las operaciones:

Mensaje de error	Explicación	Resolución

SMO-12347 [ERROR]: El servidor SnapManager no se ejecuta en la <host> del host y en la <port> de puertos. Ejecute este comando en un host que ejecuta el servidor SnapManager.	Al configurar el perfil, debe introducir información sobre el host y el puerto. Sin embargo, SnapManager no puede realizar estas operaciones porque el servidor SnapManager no está en ejecución en el host y el puerto especificados.	Introduzca el comando en un host que ejecuta el servidor SnapManager. Puede comprobar el puerto con el comando lsnrctl status y ver el puerto en el que se ejecuta la base de datos. Si es necesario, cambie el puerto del comando backup.

Ejecución de componentes de proceso (serie 13,000)

En la siguiente tabla se muestran los errores comunes asociados con el componente de proceso de SnapManager:

Mensaje de error	Explicación	Resolución
SMO-13083: El patrón de Snapname con el valor "x" contiene caracteres que no son letras, números, guion bajo, guion y llaves.	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha incluido caracteres especiales que no están permitidos.	Quite caracteres especiales que no sean letras, números, guion bajo, guion y corchetes.
SMO-13084: El patrón de Snapname con el valor "x" no contiene el mismo número de llaves izquierda o derecha.	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, las llaves izquierda y derecha no coinciden.	Introduzca los corchetes de apertura y cierre coincidentes en el patrón de Snapname.
SMO-13085: El patrón de Snapname con el valor "x" contiene un nombre de variable no válido de "y".	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha incluido una variable que no está permitida.	Elimine la variable ofensor. Para ver una lista de variables aceptables, consulte Nomenclatura de copias Snapshot.
El patrón de Snapname de SMO-13086 con el valor "x" debe contener la variable "smid".	Al crear un perfil, ha personalizado el patrón Snapname; sin embargo, ha omitido la variable smid necesaria.	Inserte la variable smid necesaria.
SMO-13902: Error al iniciar la división del clon.	Puede haber varios motivos para este error: • No hay espacio en el volumen. • SnapDrive no está en ejecución. • El clon puede ser un clon de la LUN. • El volumen de FlexVol tiene copias snapshot restringidas.	Compruebe el espacio disponible en el volumen con el comando clone Split-Estimate. Confirmar que el volumen FlexVol no tiene copias snapshot restringidas.

SMO-13904: Error de resultado de división de clones.	Esto podría deberse a un fallo en el SnapDrive o el sistema de almacenamiento.	Intente trabajar con un clon nuevo.
SMO-13906: Operación de división en ejecución para los clones etiqueta-clone o IDclone-id	Intenta dividir un clon que ya está dividido.	El clon ya está dividido y se eliminarán los metadatos relacionados con los clones.
SMO-13907: Operación de división en ejecución para los clones etiqueta-clone o IDclone-id	Está intentando dividir un clon que está en proceso de división.	Debe esperar hasta que finalice la operación de división.

Mensajes de error asociados con utilidades de SnapManager (serie 14,000)

En la siguiente tabla se muestran los errores comunes asociados con las utilidades de SnapManager:

Mensaje de error	Explicación	Resolución
SMO-14501: El ID de correo no puede estar vacío.	No ha introducido la dirección de correo electrónico.	Introduzca una dirección de correo electrónico válida.
SMO-14502: El asunto del correo no puede estar vacío.	No ha introducido el asunto del correo electrónico.	Introduzca el asunto del correo electrónico que corresponda.
SMO-14506: El campo del servidor de correo no puede estar vacío.	No se introdujo el nombre de host ni la dirección IP del servidor de correo electrónico.	Introduzca el nombre de host o la dirección IP del servidor de correo válido.
SMO-14507: El campo Puerto de correo no puede estar vacío.	No ha introducido el número de puerto de correo electrónico.	Introduzca el número de puerto del servidor de correo electrónico.
SMO-14508: Del ID de correo no puede estar en blanco.	No ha introducido la dirección de correo electrónico del remitente.	Introduzca una dirección de correo electrónico del remitente válida.
SMO-14509: El nombre de usuario no puede estar vacío.	Habilitó la autenticación y no proporcionó el nombre de usuario.	Introduzca el nombre de usuario de autenticación por correo electrónico.
SMO-14510: La contraseña no puede estar vacía. Introduzca la contraseña.	Habilitó la autenticación y no proporcionó la contraseña.	Introduzca la contraseña de autenticación por correo electrónico.
SMO-14550: Estado del correo electrónico: <success/failure>.	El número de puerto, el servidor de correo o la dirección de correo electrónico del receptor no son válidos.	Proporcione los valores adecuados durante la configuración del correo electrónico.

SMO-14559: Error al enviar una notificación de correo electrónico: <error>.	Esto podría deberse a un número de puerto no válido, a un servidor de correo no válido o a una dirección de correo del destinatario no válida.	Proporcione los valores adecuados durante la configuración del correo electrónico.
SMO-14560: Error de notificación: La configuración de la notificación no está disponible.	Error en el envío de notificaciones porque la configuración de notificación no está disponible.	Agregar configuración de notificación.
SMO-14565: Formato de hora no válido. Introduzca el formato de hora en HH:mm.	Introdujo la hora en un formato incorrecto.	Introduzca la hora en el formato: hh:mm.
SMO-14566: Valor de fecha no válido. El rango de fechas válido es 1-31.	La fecha configurada es incorrecta.	La fecha debe estar entre 1 y 31.
SMO-14567: Valor del día no válido. El rango de días válido es de 1 a 7.	El día configurado es incorrecto.	Introduzca el intervalo de días del 1 al 7.
SMO-14569: El servidor no pudo iniciar la programación de notificaciones de resumen.	El servidor SnapManager se cerró por motivos desconocidos.	Inicie el servidor SnapManager.
SMO-14570: Notificación resumida no disponible.	No ha configurado la notificación de resumen.	Configure la notificación de resumen.
SMO-14571: No se pueden habilitar las notificaciones de perfil y de resumen.	Ha seleccionado las opciones de notificación de perfil y resumen.	Habilite la notificación de perfil o la notificación de resumen.
SMO-14572: Proporcione un éxito o una opción de fallo para las notificaciones.	No ha habilitado las opciones de éxito o fallo.	Debe seleccionar Success o Failure Option o both.

Mensajes de error comunes de SnapDrive para UNIX

En la siguiente tabla se muestran los errores comunes relacionados con SnapDrive para UNIX:

Mensaje de error	Explicación
0001-136 error de administrador: No se puede iniciar sesión en el archivador: <filer> establezca un nombre de usuario y/o una contraseña para <filer>	Error de configuración inicial

0001-382 error de administrador: Se ha producido un error en la detección multivía	Error de detección de LUN
0001-462 error de administrador: No se pudo desconfigurar la multivía para <LUN>: Spd5: No se puede detener el dispositivo. Dispositivo ocupado.	Error de detección de LUN
0001-476 error de administrador: No se puede detectar el dispositivo asociado…	Error de detección de LUN
0001-680 error de administrador: El SO del host requiere una actualización de los datos internos para permitir la creación o la conexión de la LUN. Use "SnapDrive config prepare lun" o actualice esta información manualmente…	Error de detección de LUN
0001-710 error de administrador: Error de actualización del SO de LUN…	Error de detección de LUN
0001-817 error de administrador: No se pudo crear el clon de volumen… : FlexClone no tiene licencia	Error de configuración inicial
0001-817 error de administrador: No se pudo crear el clon de volumen… : Error en la solicitud porque no se puede garantizar el espacio para el clon.	Problema de espacio
0001-878 error de administrador: No se ha encontrado el asistente de HBA. Los comandos que implican las LUN deben fallar.	Error de detección de LUN
SMO-12111: Error al ejecutar el comando SnapDrive "<comando SnapDrive>": <error de SnapDrive>	Error genérico de SnapDrive para UNIX

Información relacionada

Nomenclatura de copias Snapshot

Guía de instalación y administración

Esta guía describe cómo instalar y administrar SnapManager 3.4.2 para Oracle en un entorno de Windows, incluidos cómo instalar, actualizar, desinstalar y configurar el producto, cómo realizar backup, restaurar y clonar bases de datos.

Qué es para Oracle

SnapManager proporciona las herramientas necesarias para realizar la gestión de datos condicionada por políticas, programar y crear backups de bases de datos regulares, restaurar datos de estos backups en caso de pérdida de datos o desastre, y crear clones de bases de datos. Es posible crear backups en el almacenamiento primario y crear backups protegidos en el almacenamiento secundario mediante scripts de procesamiento posterior.

SnapManager aprovecha las tecnologías de NetApp al integrarse con las versiones más recientes de las bases de datos. SnapManager se integra con las siguientes aplicaciones y tecnologías de NetApp:

- SnapDrive automatiza las tareas de aprovisionamiento del almacenamiento y simplifica el proceso de creación de copias Snapshot del almacenamiento sin errores consistentes con el host.
- Snapshot (una función de Data ONTAP) crea copias de un momento específico de la base de datos.
- SnapVault (una función con licencia de Data ONTAP) aprovecha los backups basados en disco para realizar backups y recuperaciones de bases de datos fiables y con una sobrecarga mínima.
- SnapMirror (una función con licencia de Data ONTAP) replica los datos de base de datos a través de una red global a alta velocidad de forma sencilla, fiable y rentable.
- SnapRestore (una función con licencia de Data ONTAP) recupera una base de datos completa en segundos, independientemente de la capacidad o del número de archivos.
- FlexClone (una función con licencia de Data ONTAP) ayuda a crear clones de bases de datos rápidos y con gestión eficiente del espacio a partir de los backups de Snapshot.

SnapManager funciona con todos los protocolos SAN (FC e iSCSI).

SnapManager también se integra con la tecnología original de Oracle, como Oracle Recovery Manager (RMAN).

Qué hace SnapManager para Oracle

SnapManager para Oracle simplifica y automatiza el backup, la recuperación y el clonado de bases de datos aprovechando las tecnologías de copias Snapshot, SnapRestore y FlexClone.

SnapManager ofrece las siguientes ventajas a los administradores de bases de datos:

- Trabajar con perfiles de base de datos
  - Puede organizar y conservar la información del host y la base de datos en los perfiles.

    Al iniciar un backup basado en un perfil, puede reutilizar la información en lugar de volver a introducirla para cada backup. SnapManager también le permite supervisar las operaciones rápidamente

mediante el uso de perfiles.

  - En el perfil, puede definir los patrones de nomenclatura de las copias Snapshot y escribir el texto personalizado (prefijo o sufijo), de modo que todas las copias Snapshot puedan usar la misma convención de nomenclatura que cumpla las políticas empresariales.
  - No necesita conocer el nombre del sistema de almacenamiento, ya que los archivos de la base de datos se asignan automáticamente al almacenamiento asociado.
  - Al crear un nuevo perfil, es posible especificar la opción de separar el backup del registro de archivos del backup del archivo de datos.

    También puede actualizar el perfil existente para separar la copia de seguridad del archivo de datos.

- Se realiza la operación de backup de la base de datos
  - Backup de bases de datos completas y parciales
    - Se puede crear rápidamente un backup completo o parcial de manera que ahorra espacio, lo que le permite realizar backups con mayor frecuencia.

      El backup completo de la base de datos contiene todos los archivos de datos, los archivos de control y los archivos de registro de archivos en un único backup.

  El backup parcial de las bases de datos contiene los archivos de datos o espacios de tablas especificados, todos los archivos de control y todos los archivos de registro de archivos.

  - Puede proteger los backups en el almacenamiento secundario mediante secuencias de comandos de posprocesamiento.
  - Se pueden programar backups por hora, semana, día, mes o ilimitado.
    - Separe las copias de seguridad de los archivos de datos y los archivos de registro de archivo
  - SnapManager (3.2 o posterior) permite realizar un backup de los archivos de datos y los archivos de registro de archivos por separado. Para realizar esta operación, debe especificar la opción de separar los archivos de registro de archivos mientras crea o actualiza el perfil.
  - Puede especificar el número y la duración para el cual se retendrán los backups de archivos de datos, en la política de retención.
  - Es posible especificar la duración de los backups de archivos de registro de archivos que se retendrán en la retención de registros de archivo.
  - SnapManager (3.2 o posterior) también consolida los backups de registros de archivos a un número mínimo de backups, ya que libera los backups de registros de archivos con archivos duplicados y conserva únicamente los backups de los registros de archivos con archivos únicos de registro de archivos. Sin embargo, esta consolidación se puede deshabilitar opcionalmente.
- Gestión de los archivos archive log
  - SnapManager (3.2 o posterior) permite comprimir los archivos de registro de archivos desde los destinos de registro de archivos.

    El espacio ocupado por los archivos de registro de archivos prados se libera cuando se purgan los backups de registros de archivos que contienen estos archivos de registro de archivos.

  - SnapManager garantiza que se realice un backup de los archivos de registro de archivos antes de eliminarlos de los destinos de registros de archivos.

    No se reducen los archivos de registro de archivos, que no se incluyen en el backup.

- SnapManager garantiza que los archivos de registro de archivos se envíen a la base de datos Data Guard en espera al mismo tiempo que elimina los archivos de registro de archivos de una base de datos Data Guard primaria.
- SnapManager garantiza que el proceso de captura de secuencias de Oracle captura los archivos de registro de archivos, si los hubiera.
- Recomendación
  - Para gestionar el espacio de destino del registro de archivos de forma eficaz, debe crear los backups del registro de archivos y abrir los archivos de registro de archivos junto con él.
- SnapManager consolida los backups de registros de archivos para contener un número mínimo de backups mediante la liberación de los backups de registros de archivos con archivos de registro de archivos duplicados y la retención únicamente de los backups de registros de archivos con archivos de registro únicos.

  Sin embargo, esta consolidación se puede deshabilitar opcionalmente. Se liberan los backups de registros de archivos, que contienen archivos de registro de archivos duplicados y se conserva un único backup con registros de archivos únicos.

- Se ejecuta la operación de restauración de bases de datos
  - Es posible realizar operaciones de restauración basadas en archivos.

    También es posible ver una vista previa de las operaciones de restauración y obtener un análisis de archivo por archivo de las operaciones de restauración antes de ejecutar la operación.

  - Puede reducir el tiempo medio de restauración de una base de datos mediante SnapRestore.
  - SnapManager (3.2 o posterior) permite recuperar la base de datos automáticamente mediante los archivos de registro de archivos del backup, incluso si no hay archivos del registro de archivos disponibles en el destino del registro de archivos.

    SnapManager (3.2 o posterior) también proporciona un método para recuperar la base de datos utilizando los archivos de registro de archivos de la ubicación externa hasta cierto punto.

- Clonar una base de datos para realizar pruebas y desarrollo
  - Puede crear un clon de una base de datos para que la base de datos pueda configurarse fuera del entorno de producción.

    Por ejemplo, puede clonar en los entornos de desarrollo y prueba para probar actualizaciones a sistemas vitales.

  - Es posible clonar una base de datos en un sistema de almacenamiento primario.
  - SnapManager (3.2 o posterior) permite clonar los backups de archivos de datos con los archivos de registro de archivos disponibles en el backup.
    - Es posible clonar los backups de archivos de datos solo cuando se realiza el backup de registros de archivos junto con él.
    - También es posible clonar los backups de archivos de datos si los archivos de registro de archivos están disponibles en los backups de registros de archivos que se realizan por separado en cierta medida.
    - También es posible clonar los backups de archivos de datos de una base de datos independiente en cierta medida con los archivos de registro de archivos desde cualquier ubicación externa a la que pueda acceder Oracle.

        - Si los backups están disponibles desde una ubicación externa, puede especificar la ubicación externa durante la clonado para recuperar la base de datos clonada en un estado coherente.
    - No se admite la clonado de backups de solo registro de archivos.
- Generales
    - Integre con herramientas de Oracle existentes, como Recovery Manager (RMAN).

SnapManager ofrece las siguientes ventajas a los administradores de almacenamiento:

- Admite diferentes protocolos SAN.
- Permite optimizar los backups según el tipo de backup (completo o parcial) que mejor se adapte a su entorno.
- Creación de backups de bases de datos con mejor aprovechamiento del espacio.
- Crea clones con gestión eficiente del espacio.

SnapManager también funciona con las siguientes funciones de Oracle:

- SnapManager puede catalogar sus backups con RMAN de Oracle.

  Si utiliza RMAN, un DBA puede utilizar las copias de seguridad de SnapManager y conservar el valor de todas las funciones de RMAN, como la restauración a nivel de bloque. SnapManager permite a RMAN utilizar las copias snapshot cuando realiza la recuperación o restauración. Por ejemplo, puede utilizar RMAN para restaurar una tabla dentro de un espacio de tablas y realizar restauraciones y recuperaciones completas de bases de datos y tablespaces a partir de copias Snapshot realizadas por SnapManager. El catálogo de recuperación de RMAN no debe estar en la base de datos de la que se está realizando la copia de seguridad.

Integración con otras aplicaciones y tecnologías de NetApp

SnapManager para Oracle es un producto independiente que integra las funciones de otros productos de NetApp para permitir backups rápidos que solo requieren una pequeña cantidad de espacio.

SnapManager se integra con las siguientes aplicaciones y tecnologías de NetApp:

Aplicaciones y tecnologías	Descripción
SnapDrive	SnapManager utiliza SnapDrive para crear copias Snapshot del almacenamiento. Las copias Snapshot garantizan que los backups ocupan poco espacio y son más rápidos que los backups de disco a disco.
FlexClone (una función con licencia de Data ONTAP)	SnapManager utiliza la función FlexClone para crear clones de backups con rapidez y gestión eficiente del espacio.
Snapshot (una función de Data ONTAP)	La tecnología Snapshot crea copias puntuales de la base de datos.

SnapRestore (función con licencia de Data ONTAP)	SnapManager reduce el tiempo medio de recuperación de una base de datos mediante SnapRestore. SnapRestore puede recuperar archivos independientes en un volumen de varios terabytes para que las operaciones se puedan reanudar rápidamente.
SnapVault (función con licencia de Data ONTAP)	SnapVault aprovecha los backups basados en disco para realizar backups y recuperaciones de bases de datos fiables y de baja sobrecarga.
SnapMirror (función con licencia de Data ONTAP)	SnapMirror replica los datos de bases de datos a alta velocidad a través de una red global de forma sencilla, fiable y rentable.

Ventajas de usar SnapManager

Puede utilizar SnapManager para Oracle para realizar diferentes tareas en las bases de datos y gestionar los datos con eficiencia.

SnapManager para Oracle funciona con sistemas de almacenamiento y permite realizar las siguientes tareas:

- Crear backups con un uso eficiente del espacio en el almacenamiento primario o secundario y programar backups.

  Se pueden crear backups completos y parciales de bases de datos y aplicar políticas de duración de retención.SnapManager (3.2 o posterior) permite crear backups solo de los archivos de datos y los registros de archivos.

  - SnapManager (3.2 o posterior) le permite realizar un procesamiento previo o posterior antes o después de las operaciones de backup y restauración.
  - SnapManager (3.2 o posterior) permite proteger los backups mediante las secuencias de comandos postprocesamiento.
- Restaure bases de datos completas o parciales mediante la operación de restauración basada en archivos.
- Restaurar y recuperar backups de bases de datos automáticamente.

  SnapManager (3.2 o posterior) permite restaurar y recuperar backups de bases de datos de forma automática. SnapManager recupera automáticamente la base de datos restaurada mediante la detección, el montaje y la aplicación de los archivos de registro de archivos a partir de los backups.

- Reducir los archivos de registro de archivos de los destinos de registro de archivos cuando se crean backups solo para los registros de archivos.
- Conserve la cantidad mínima de backups de registros de archivos automáticamente conservando solo los backups con archivos de registro de archivos únicos.
- Realizar un seguimiento de los detalles de las operaciones y generar informes por host, perfil, backup o clon.
- Compruebe el estado del backup.

- Mantener el historial de operaciones de SnapManager asociadas a un perfil.
- Crear clones de backups con gestión eficiente del espacio en el almacenamiento principal.

Crear backups usando copias de Snapshot

SnapManager permite crear backups en el almacenamiento primario (local) y en el almacenamiento secundario (remoto) mediante scripts de posprocesamiento.

Los backups que se crean como copias Snapshot son copias virtuales de la base de datos y se almacenan en el mismo medio físico que la base de datos. Por consiguiente, la operación de backup requiere menos tiempo y mucho menos espacio que los backups completos de disco a disco. SnapManager permite realizar el backup de los siguientes elementos:

- Todos los archivos de datos, los archivos de registro de archivo y los archivos de control
- Los archivos de datos o espacios de tablas seleccionados, todos los archivos de registro de archivo y los archivos de control

SnapManager 3.2 o posterior le permite realizar, opcionalmente, el backup de lo siguiente:

- Todos los archivos de datos y los archivos de control
- Los archivos de datos o tablespaces seleccionados junto con los archivos de control
- Archivos de registro de archivo

> Los archivos de datos, los archivos de registro de archivos y los archivos de control pueden ubicarse en diferentes sistemas de almacenamiento, volúmenes de sistema de almacenamiento y números de unidad lógica (LUN). También se puede usar SnapManager para realizar backup de una base de datos cuando hay varias bases de datos en el mismo volumen o LUN.

Por qué debe prune los archivos de registro de archivos

SnapManager para Oracle permite eliminar archivos de registro de archivos del sistema de archivos activo de del que ya se ha realizado un backup.

Eliminar permite a SnapManager crear backups de diferentes archivos de registro de archivos. Eliminar, junto con la política de retención de backups, libera espacio en los registros de archivos cuando se purgan los backups.

> No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos. Si especifica la ubicación del registro de archivos en el área de recuperación flash, debe asegurarse de especificar también la ubicación del registro de archivos en el parámetro archive_log_dest.

Consolidación de registros de archivo

SnapManager (3.2 o posterior) para Oracle consolida los backups de registros de archivos a fin de mantener una cantidad mínima de backups para los archivos de registro de archivos. SnapManager para Oracle identifica y libera los backups que contienen archivos de registros de archivos que son subconjuntos de otros backups.

Restauración total o parcial de bases de datos

SnapManager proporciona la flexibilidad necesaria para restaurar bases de datos completas, espacios de tablas específicos, archivos, archivos de control o una combinación de estas entidades. SnapManager le permite restaurar datos mediante un proceso de restauración basado en archivos.

SnapManager permite a los administradores de bases de datos obtener una vista previa de las operaciones de restauración. La función de vista previa permite a los administradores de bases de datos ver cada operación de restauración archivo por archivo.

Los administradores de bases de datos pueden especificar el nivel en el que SnapManager restaura y recupera la información cuando se ejecutan operaciones de restauración. Por ejemplo, los administradores de bases de datos pueden restaurar y recuperar datos en momentos específicos. El punto de restauración puede ser una fecha y hora, o un número de cambio de sistema (SCN) de Oracle.

Los administradores de bases de datos pueden usar SnapManager para restaurar la base de datos y usar otra herramienta para recuperar la información. Los administradores de bases de datos no tienen que usar SnapManager para ambas operaciones.

SnapManager (3.2 o posterior) permite restaurar y recuperar backups de bases de datos de forma automática sin intervención del administrador de base de datos. Es posible usar SnapManager para crear backups de registros de archivo, y luego usarlos para restaurar y recuperar los backups de bases de datos. Aunque los archivos de registro de archivo del backup se gestionen en una ubicación de un registro de archivo externo, puede especificar esa ubicación externa para que los registros de archivos puedan ayudar a recuperar la base de datos restaurada.

Comprobar el estado del backup

SnapManager puede confirmar la integridad del backup mediante las operaciones estándar de verificación de backup de Oracle.

Los administradores de bases de datos pueden realizar la verificación como parte de la operación de backup o al mismo tiempo. Los administradores de bases de datos pueden configurar la operación de verificación para que se produzca durante un tiempo de pico de actividad cuando la carga en los servidores host es menor o durante un período de mantenimiento programado.

Clones de backups de bases de datos

SnapManager utiliza la tecnología FlexClone para crear un clon modificable de un backup de base de datos con un uso eficiente del espacio. Es posible modificar un clon sin cambiar el origen de backup.

Quizás sería conveniente clonar bases de datos para permitir pruebas o actualizaciones en entornos no productivos. Puede clonar una base de datos que reside en el primario. Puede ubicarse un clon en el mismo host o en otro que la base de datos.

La tecnología FlexClone permite a SnapManager utilizar copias snapshot de la base de datos para evitar crear una copia física completa de disco a disco. Las copias Snapshot requieren menos tiempo de creación y ocupan mucho menos espacio que las copias físicas.

Consulte la documentación de Data ONTAP para obtener más información sobre la tecnología FlexClone.

Información relacionada

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

Realizar un seguimiento de los detalles y generar informes

SnapManager reduce el nivel de detalle que los administradores de las bases de datos necesitan para realizar un seguimiento del estado de las diferentes operaciones mediante la oferta de métodos para supervisar las operaciones desde una única interfaz.

Una vez que los administradores especifican qué bases de datos deben realizarse backups, SnapManager identifica automáticamente los archivos de la base de datos para el backup. SnapManager muestra información sobre repositorios, hosts, perfiles, backups y clones. Es posible supervisar las operaciones en hosts o bases de datos específicas.

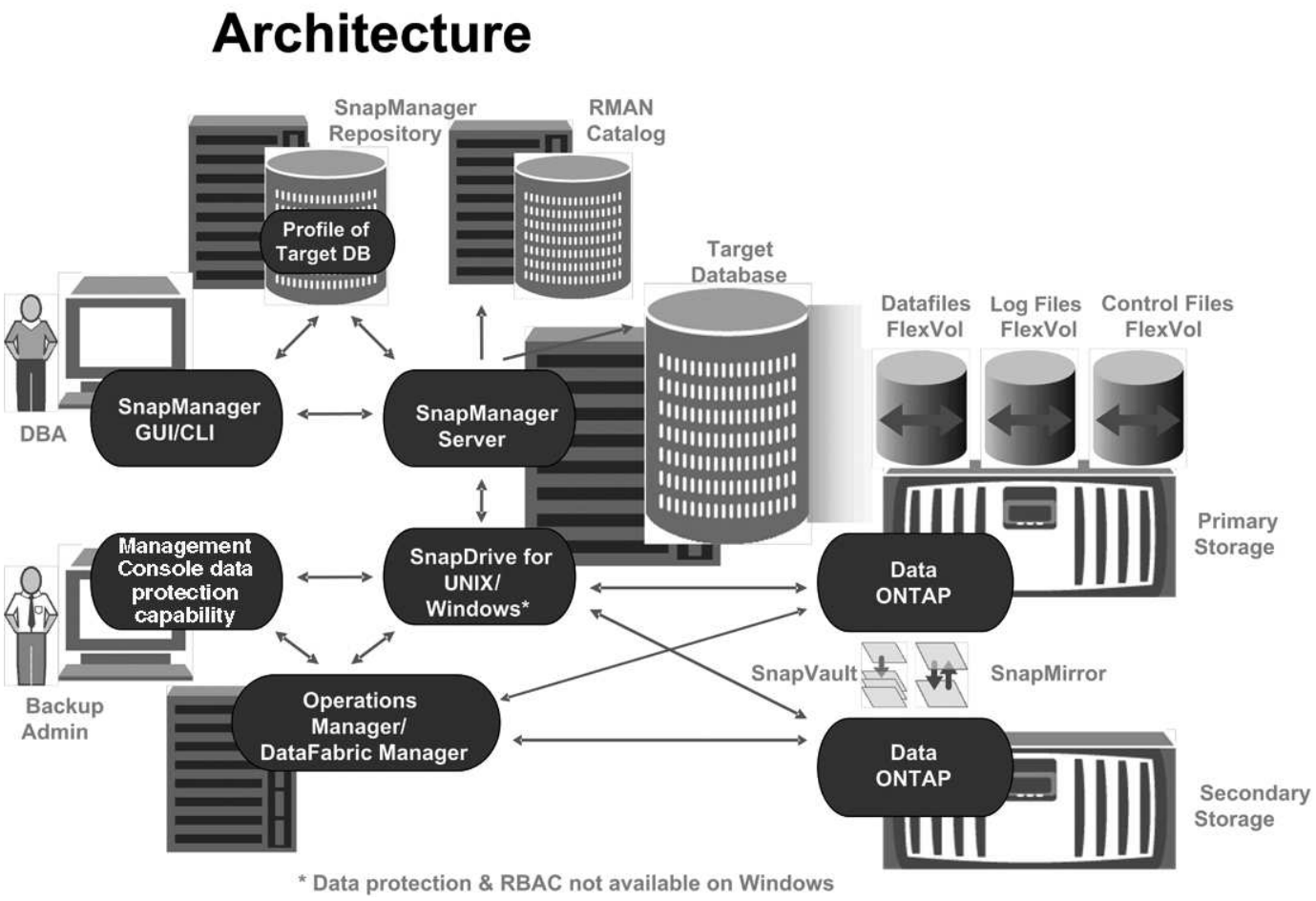
En qué consiste la arquitectura de SnapManager para Oracle

La arquitectura de SnapManager para Oracle incluye muchos componentes, como el host, el cliente y el repositorio de SnapManager para Oracle. Otros componentes son los sistemas de almacenamiento primario y secundario y otros productos de NetApp.

La arquitectura de SnapManager para Oracle incluye los siguientes componentes arquitectónicos:

- Host SnapManager
- Interfaz gráfica de usuario o interfaz de línea de comandos de SnapManager
- Repositorio de SnapManager
- Sistema de almacenamiento primario
- Sistemas de almacenamiento secundario
- SnapDrive para Windows

En la siguiente imagen se muestra la arquitectura de SnapManager para Oracle y los componentes relacionados:



Host SnapManager

El host SnapManager es un servidor de Windows que también ejecuta otros productos de NetApp.

El host de SnapManager se instala con los siguientes productos:

- SnapDrive para Windows
- Utilidades de host

El host de SnapManager se ejecuta como servicio.

Interfaces gráficas de usuario y de línea de comandos de SnapManager

El cliente SnapManager incluye tanto una interfaz gráfica de usuario (GUI) como una interfaz de línea de comandos (CLI).

Repositorio de SnapManager

El repositorio almacena información relacionada con las diferentes operaciones de SnapManager; por ejemplo, la hora de los backups, los espacios de tablas y los archivos de datos de los que se ha realizado backup, los sistemas de almacenamiento utilizados, los clones realizados y las copias Snapshot creadas.

La base de datos del repositorio no puede existir en la misma base de datos y tampoco puede formar parte de la misma base de datos de la que se realiza el backup de SnapManager. Esto se debe a que el repositorio almacena los nombres de las copias Snapshot de la base de datos creadas durante las operaciones de backup. El repositorio debe crearse en una base de datos diferente a la de la base de datos del que se va a realizar backup. Esto significa que debe tener al menos dos bases de datos: La base de datos del repositorio de SnapManager y la base de datos de destino gestionada por SnapManager. Cuando se ejecutan los servicios SnapManager, ambas bases de datos deben estar en funcionamiento.

> No se debe realizar ninguna operación de SnapManager mediante la interfaz gráfica de usuario o la interfaz de línea de comandos cuando la base de datos del repositorio está inactiva.

SnapDrive en el servidor SnapManager

SnapManager utiliza SnapDrive para Windows para crear copias Snapshot del sistema de almacenamiento. SnapDrive reside en el mismo servidor que SnapManager.

Qué repositorios son

SnapManager organiza la información en perfiles, que a continuación se asocian con repositorios. Los perfiles contienen información acerca de la base de datos que se está gestionando, mientras que el repositorio contiene datos acerca de las operaciones que se realizan en los perfiles.

El repositorio registra el momento en que se realizó un backup, qué archivos se hicieron de backup y si se creó un clon a partir del backup. Cuando los administradores de bases de datos restauran una base de datos o recuperan una parte del mismo, SnapManager consulta el repositorio para determinar qué se ha realizado un backup.

Como el repositorio almacena los nombres de las copias Snapshot de la base de datos creadas durante las operaciones de backup, la base de datos del repositorio no puede existir en la misma base de datos y tampoco puede formar parte de la misma base de datos de la que se realiza el backup de SnapManager. Debe tener al menos dos bases de datos (la base de datos del repositorio de SnapManager y la base de datos de destino que gestiona SnapManager) en funcionamiento cuando se ejecutan operaciones de SnapManager.

Si intenta abrir la interfaz gráfica de usuario (GUI) cuando la base de datos del repositorio está inactiva, se registra el siguiente mensaje de error en el archivo sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: No se han producido más datos para leer desde el socket. Además, se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva. Para obtener más información acerca de los diferentes mensajes de error, consulte *solución de problemas conocidos*.

Es posible usar cualquier nombre de host, nombre de servicio o nombre de usuario válido para realizar operaciones. Para que un repositorio admita operaciones SnapManager, el nombre de usuario y el nombre de servicio del repositorio sólo deben contener los siguientes caracteres: Caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-), guión bajo (_) y punto (.).

El puerto de repositorio puede ser cualquier número de puerto válido y el nombre de host del repositorio puede ser cualquier nombre de host válido. El nombre de host debe estar formado por caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-) y punto (.), pero no un guión bajo (_).

El repositorio debe crearse en una base de datos de Oracle. La base de datos que utiliza SnapManager debe configurarse de acuerdo con los procedimientos de Oracle para la configuración de la base de datos.

Un único repositorio puede contener información acerca de varios perfiles; sin embargo, cada base de datos normalmente se asocia a un único perfil. Puede tener varios repositorios, donde cada repositorio contiene varios perfiles.

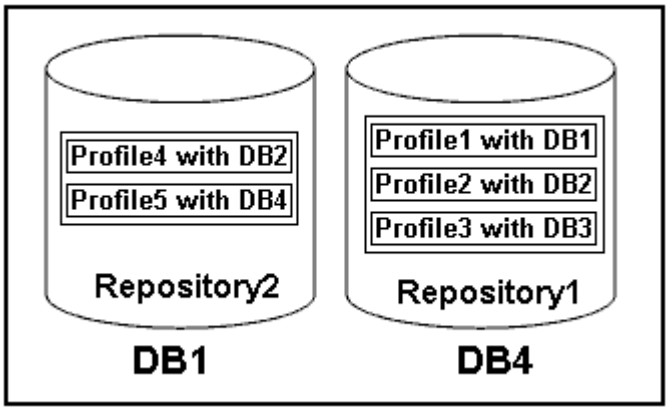
Qué perfiles son

SnapManager utiliza perfiles para almacenar la información necesaria para realizar operaciones en una base de datos determinada. Un perfil contiene información sobre la base de datos, incluidas sus credenciales, backups y clones. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos.

Un perfil sólo puede hacer referencia a una base de datos. Más de un perfil puede hacer referencia a la misma base de datos. No es posible acceder a los backups creados con un perfil desde otro perfil, aunque ambos perfiles hagan referencia a la misma base de datos.

La información del perfil se almacena en un repositorio. El repositorio contiene información de perfil de la base de datos e información sobre las copias de Snapshot que sirven como backup de base de datos. Las copias Snapshot reales se almacenan en el sistema de almacenamiento. Los nombres de las copias Snapshot se almacenan en el repositorio que contiene el perfil de esa base de datos. Cuando se realiza una operación en una base de datos, debe seleccionar el perfil en el repositorio.

La siguiente figura muestra cómo los repositorios pueden contener varios perfiles, pero también que cada perfil puede definir sólo una base de datos:



En el ejemplo anterior, deleteRepository2 se encuentra en la base de datos DB1 y deleteRepository1 en la base de datos DB4.

Cada perfil contiene las credenciales de la base de datos asociada al perfil. Las credenciales permiten que SnapManager se conecte a la base de datos y trabaje con ella. Las credenciales almacenadas incluyen el nombre de usuario y las parejas de contraseñas para acceder al host, al repositorio, a la base de datos y a la información de conexión necesaria si utiliza Oracle Recovery Manager (RMAN).

No se puede acceder a un backup que se creó con un perfil de otro perfil, incluso si los dos perfiles están asociados con la misma base de datos. SnapManager coloca un bloqueo en la base de datos para evitar que se realicen dos operaciones incompatibles a la vez.

Perfil para crear copias de seguridad completas y parciales

Puede crear perfiles para realizar copias de seguridad completas o parciales.

Los perfiles que se especifican para crear las copias de seguridad completas y parciales contienen tanto los archivos de datos como los archivos de registro de archivos. SnapManager no permite que dichos perfiles separen los backups de registros de archivo de los backups del archivo de datos. Los backups completos y parciales se retienen en función de las políticas de retención de backup existentes. Puede programar copias de seguridad completas y parciales en función del tiempo y la frecuencia que mejor le convenga.

Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad de sólo registro de archivos

SnapManager (3.2 o posterior) permite crear perfiles para realizar backups de los archivos de registro de archivos independientemente de los archivos de datos. Después de usar el perfil para separar los tipos de backup, es posible crear backups de solo los archivos de datos o backups de solo registros de archivos de la base de datos. También es posible crear un backup que contenga los archivos de datos y los archivos de registro de archivos juntos.

La política de retención se aplica a todos los backups de la base de datos cuando no están separados los backups de registros de archivos. Después de separar las copias de seguridad de los registros de archivos, SnapManager permite especificar diferentes duraciones de retención .

Política de retención

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Una copia de seguridad caduca cuando su antigüedad supera el período de retención establecido para su clase de retención y la cantidad de backups supera el número de retención. Por ejemplo, si el número de backup es 15 (lo que significa que SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups más antiguos, correctos y elegibles caducan.

Duración de la retención del registro de archivo

Una vez separados los backups de los registros de archivos, se retienen en función de la duración de la retención de los registros de archivos. Los backups de registros de archivo que se realizan con los backups de archivos de datos siempre se conservan junto con estos backups de archivos de datos, independientemente de la duración de la retención de registros de archivo.

Información relacionada

Gestionar perfiles para backups eficientes

Qué son los estados de operación de SnapManager

Las operaciones de SnapManager (backup, restauración y clonado) pueden estar en diferentes estados y cada estado indica el progreso de la operación.

Estado de la operación	Descripción
Correcto	La operación se ha completado correctamente.
Ejecutando	La operación se inició, pero no ha finalizado. Por ejemplo, se programa que un backup, que tarda dos minutos, se lleve a cabo a las 11:00. Al ver la ficha **Programación** a las 11:01 a.m., la operación aparece como en ejecución.

No se ha encontrado ninguna operación	La programación no se ha ejecutado o se ha eliminado la última copia de seguridad ejecutada.
Error	Error en la operación. SnapManager ha ejecutado automáticamente el proceso de anulación y ha limpiado la operación.

Eventos recuperables e irrecuperables

Un evento SnapManager recuperable tiene los siguientes problemas:

- La base de datos no se almacena en un sistema de almacenamiento que ejecuta Data ONTAP.
- SnapDrive para Windows no está instalado o no puede acceder al sistema de almacenamiento.
- SnapManager no puede crear una copia Snapshot o aprovisionar almacenamiento si el volumen no tiene espacio, se alcanzó el número máximo de copias Snapshot o se produce una excepción no prevista.

Cuando se produce un evento recuperable, SnapManager realiza un proceso de anulación e intenta devolver el host, la base de datos y el sistema de almacenamiento al estado inicial. Si el proceso de anulación falla, SnapManager trata el incidente como un evento irrecuperable.

Un evento irrecuperable (fuera de banda) se produce cuando se produce cualquiera de los siguientes acontecimientos:

- Se produce un problema con el sistema, como cuando se produce un error en un host.
- Se ha detenido el proceso SnapManager.
- Se produce un error en una operación de anulación en banda cuando el sistema de almacenamiento falla, el número de unidad lógica (LUN) o el volumen de almacenamiento están sin conexión o la red falla.

Cuando se produce un evento irrecuperable, SnapManager realiza un proceso de cancelación inmediatamente. Es posible que el host, la base de datos y el sistema de almacenamiento no regresen a los estados iniciales. Si este es el caso, debe realizar una limpieza después de que la operación SnapManager falle; para ello, elimine la copia snapshot huérfana y elimine el archivo de bloqueo de SnapManager.

Si desea eliminar el archivo de bloqueo SnapManager, desplácese a $ORACLE_HOME en el equipo de destino y elimine el archivo sm_lock_TargetDBName. Después de eliminar el archivo, debe reiniciar SnapManager para Oracle Server.

Cómo mantiene SnapManager la seguridad

Es posible realizar operaciones de SnapManager solo si cuenta con las credenciales adecuadas. La seguridad en SnapManager se rige por la autenticación de usuarios.

SnapManager mantiene la seguridad al solicitar la autenticación del usuario mediante peticiones de contraseña o al configurar credenciales de usuario. Un usuario efectivo se autentica y autoriza con el servidor SnapManager.

Las credenciales de SnapManager y la autenticación de usuario difieren significativamente de SnapManager 3.0:

- En las versiones de SnapManager anteriores a la 3.0, debe establecer una contraseña de servidor arbitraria al instalar SnapManager. Cualquier persona que desee utilizar el servidor SnapManager

necesitará la contraseña del servidor SnapManager. La contraseña del servidor SnapManager debería añadirse a las credenciales de usuario mediante el comando smo credential set -host.

- En SnapManager (3.0 y posterior), la contraseña del servidor SnapManager ha sido sustituida por la autenticación individual del sistema operativo (SO) de usuario. Si no ejecuta el cliente desde el mismo servidor que el host, el servidor SnapManager realiza la autenticación con los nombres de usuario y contraseñas del sistema operativo. Si no desea que se le soliciten las contraseñas de sistema operativo, puede guardar los datos en la caché de credenciales de usuario de SnapManager mediante el comando smo credential set -host.

> El comando smo credential set -host recuerda las credenciales cuando la propiedad host.credentials.persists del archivo smo.config está establecida en TRUE.

ejemplo

User1 y User2 comparten un perfil denominado Pro2. User2 no puede realizar una copia de seguridad de Database1 en Host1 sin permiso para acceder a Host1. User1 no puede clonar una base de datos a Host3 sin permiso para acceder a Host3.

En la siguiente tabla se describen los diferentes permisos asignados a los usuarios:

Tipo de permiso	Usuario1	Usuario2
Contraseña del host	Host1, Host2	Host2, Host3
Contraseña de repositorio	Repo. 1	Repo. 1
Contraseña de perfil	Pro1, Pro2	Profeca2

En caso de que User1 y User2 no tengan ningún perfil compartido, supongamos que User1 tiene permisos para los hosts denominados Host1 y Host2 y que User2 tiene permisos para el host denominado Host2. User2 no puede ejecutar ni siquiera los comandos que no son de perfil, como dump y verificación del sistema en Host1.

Acceso e impresión de la Ayuda en línea

La Ayuda en línea proporciona instrucciones para las tareas que puede realizar mediante la interfaz gráfica de usuario de SnapManager. La Ayuda en línea también proporciona descripciones de los campos de las ventanas y asistentes.

1. Ejecute una de las siguientes acciones:
   - En la ventana principal, haga clic en **Ayuda** > **Contenido de la Ayuda**.
   - En cualquier ventana o asistente, haga clic en **Ayuda** para ver la ayuda específica de esa ventana.
2. Utilice **Tabla de contenido** en el panel izquierdo para navegar por los temas.
3. Haga clic en el icono impresora situado en la parte superior de la ventana de ayuda para imprimir temas individuales.

Consideraciones sobre la puesta en marcha de SnapManager para Oracle

Antes de implementar SnapManager en su entorno, debe conocer el resto de aplicaciones y tecnologías que se requieren para diferentes operaciones.

La siguiente tabla enumera las diferentes aplicaciones y tecnologías:

Aplicaciones y tecnologías	Detalles
Data ONTAP	SnapManager aprovecha las herramientas y las tecnologías de NetApp, incluidas las copias Snapshot.
SnapDrive para Windows	SnapManager utiliza las funciones de SnapDrive. Debe instalar SnapDrive antes de ejecutar los servicios de SnapManager. SnapManager se ocupa de todas las interacciones con SnapDrive. SnapDrive para Windows debe estar configurado correctamente para su sistema de almacenamiento y sus opciones de protocolos.
SnapRestore	SnapManager reduce el tiempo medio de recuperación de una base de datos mediante SnapRestore. Cada sistema de almacenamiento debe tener una licencia de SnapRestore.
FlexClone	FlexClone es una función bajo licencia de Data ONTAP.
Protocolos FC e iSCSI	Necesita tener las versiones con licencia de los protocolos adecuados.

Información relacionada

"Prácticas recomendadas de SnapManager para Oracle: media.netapp.com/documents/tr-3761.pdf"

Requisitos para ejecutar SnapManager

Antes de implementar SnapManager en su entorno, debe conocer los distintos requisitos.

Antes de utilizar SnapManager, debe revisar las matrices de compatibilidad de todos los productos necesarios. También debe revisar lo siguiente:

- Matriz de compatibilidad de SnapManager y SnapDrive en la sección de interoperabilidad para obtener la información más reciente sobre versiones y revisiones de todos los hosts, sistemas de almacenamiento y otros componentes enumerados en esta sección.
- La guía de configuración de los productos FCP e iSCSI de NetApp.

SnapManager requiere versiones específicas de Oracle en algunas plataformas.

Consulte el kit de documentación para obtener más información sobre las configuraciones recomendadas para los sistemas host y de almacenamiento.

Póngase en contacto con su representante de ventas si necesita una configuración de SnapManager que no se menciona en el kit de documentación.

Información relacionada

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Hardware host compatible

Considere los requisitos de memoria, espacio en disco y CPU.

SnapManager requiere la siguiente configuración:

Funcionamiento del hardware	Requisitos de hardware
Memoria	El servidor SnapManager requiere 128 MB de memoria. Las interfaces gráficas de usuario requieren un mínimo de 512 MB de RAM para ejecutarse. Cada operación que ejecuta el servidor SnapManager requiere 48 MB de memoria adicional mientras se está ejecutando.
Espacio en disco adicional	128 MB de espacio disponible en disco para la aplicación gráfica del usuario (mínimo).
Velocidad de la CPU	Velocidad del procesador de 1.0 GHz (mínima).

Configuraciones generales admitidas

Antes de instalar SnapManager, debe conocer los requisitos de configuración generales.

SnapManager admite las siguientes configuraciones generales:

- Una configuración no en clúster donde un único host está conectado a un único sistema de almacenamiento
- Una instancia de servidor SnapManager por host
- Cualquier topología que incluya sistemas de almacenamiento que ejecuten conmutación al nodo de respaldo de la controladora Data ONTAP

Para obtener información sobre todos los tipos de almacenamiento y versiones que admite SnapManager, consulte la matriz de compatibilidad de SnapManager y SnapDrive.

Configuraciones en clúster

SnapManager funciona en configuraciones de clúster.

SnapManager es compatible con el mismo clúster de host y las mismas configuraciones que admite el producto SnapDrive y el kit de utilidades de host.

SnapManager también admite configuraciones en clúster donde hay un solo host conectado a un único sistema de almacenamiento, clústeres de hosts compatibles y sistemas de almacenamiento que ejecutan recuperación tras fallos de controladora Data ONTAP.

Compatibilidad con la versión de la base de datos y información general de la configuración

Debe conocer las distintas versiones de la base de datos y las diferentes configuraciones que admite SnapManager. Debe realizar una configuración y un diseño básicos de la base de datos para garantizar que las operaciones se realicen correctamente.

SnapManager para Oracle se integra con las versiones 10gR2 (10.2.0.5), 11gR1, 11gR2 (11.2.0.1 y 11.2.0.2), y 12*c*; con la tecnología Oracle nativa, como Recovery Manager (RMAN); y a través de los protocolos Fibre Channel (FC) y Internet Small Computer System Interface (iSCSI).

> SnapManager 3.3.1 no admite la base de datos Oracle 9i en SnapManager 3.2 y 10g R2 (anterior a 10.2.0.5).

Si va a implementar bases de datos Oracle para que las administre SnapManager para Oracle, consulte el *SnapManager para prácticas recomendadas de Oracle*.

"Prácticas recomendadas de SnapManager para Oracle: media.netapp.com/documents/tr-3761.pdf"

Diseño y configuración generales

Se puede encontrar información acerca de la distribución general de la base de datos y las configuraciones de almacenamiento recomendadas para evitar problemas relacionados con los grupos de discos, los tipos de archivo y los espacios de tablas.

- No incluya archivos de más de un tipo DE sistema DE archivos SAN en la base de datos.

  Todos los archivos que conforman una base de datos deben residir en el mismo tipo de sistema de archivos.

- SnapManager requiere un gran tamaño de bloque de 4 KB.
- Para registrar backups de SnapManager en Oracle RMAN, debe crear perfiles habilitados para RMAN.

A continuación se muestran algunas directrices para la separación de volúmenes:

- Los archivos de datos de una sola base de datos deben estar en el volumen.
- Debe utilizar volúmenes independientes para cada una de las siguientes clasificaciones de archivos: Archivos binarios de base de datos, archivos de datos, archivos redo log en línea, archivos redo log archivados y archivos de control.
- No es necesario crear un volumen separado para los archivos de base de datos temporales, ya que

SnapManager no realiza backups de archivos de base de datos temporales.

Para obtener más información, consulte *SnapManager for Oracle Best Practices*.

Información relacionada

"Prácticas recomendadas de SnapManager para Oracle: media.netapp.com/documents/tr-3761.pdf"

Ejemplos de distribuciones de volúmenes de base de datos

Puede consultar ejemplos de diseños de volumen de base de datos para obtener ayuda en la configuración de la base de datos.

Bases de datos de instancia única

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_sid	Sí	Apagado
Archivos de datos temporales	oratemp_sid	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_sid (multiplexado) Oralog02_sid (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Sí	Apagado

Limitaciones al trabajar con SnapManager

Debe conocer las situaciones y las limitaciones que pueden afectar a su entorno.

Limitaciones relacionadas con diseños y plataformas de bases de datos

- SnapManager admite archivos de control en un sistema de archivos y no admite archivos de control en dispositivos RAW.
- SnapManager funciona en un entorno de cluster Microsoft (MSCS), pero no reconoce el estado de la configuración MSCS (activo o pasivo) y no transfiere la administración activa de un repositorio a un servidor en espera en un clúster MSCS.

- La base de datos del repositorio puede existir en un host al que se puede acceder mediante más de una dirección IP.

  Si para acceder al repositorio se utiliza más de una dirección IP, se crea el archivo de programación para cada una de las direcciones IP. Si se crea la copia de seguridad de la programación para un perfil (por ejemplo, perfil A) bajo una de las direcciones IP (por ejemplo, IP1), se actualizará el archivo de planificación para sólo esa dirección IP. Si se accede al perfil A desde otra dirección IP (por ejemplo, IP2), la copia de seguridad programada no aparece porque el archivo de programación de IP2 no tiene una entrada para la programación que se creó en IP1.

  Puede esperar a que la programación se active desde esa dirección IP y el archivo de programación que se actualizará o puede reiniciar el servidor.

Limitaciones relacionadas con la configuración de SnapManager

- SnapManager se puede configurar para catalogar backups de bases de datos con RMAN.

  Si se utiliza un catálogo de recuperación de RMAN, el catálogo de recuperación debe estar en una base de datos diferente a la base de datos de la que se realiza el backup.

- SnapManager admite bases de datos en sistemas de almacenamiento de MultiStore con los siguientes requisitos:
  - Debe configurar SnapDrive para establecer contraseñas para los sistemas de almacenamiento MultiStore.
  - SnapDrive no puede crear una copia snapshot de una LUN o un archivo que reside en un qtree de un sistema de almacenamiento de MultiStore si el volumen subyacente no está en el mismo sistema de almacenamiento de MultiStore.
- SnapManager no admite el acceso a dos servidores SnapManager que se ejecutan en puertos diferentes desde un único cliente (tanto desde la CLI como desde la GUI).

  Los números de puerto deben ser los mismos en los hosts remotos y destino.

- Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

  Es necesario verificar que la base de datos del repositorio esté en ejecución cuando se realiza cualquier operación de SnapManager.

- SnapManager no es compatible con la movilidad de particiones activas (LPM) ni con la movilidad de aplicaciones activas (LAM).
- SnapManager no es compatible con Oracle Wallet Manager ni con el cifrado de datos transparente (TDE).
- SnapManager no admite configuraciones MetroCluster en entornos de asignación de dispositivos sin formato (RDM), ya que las configuraciones de MetroCluster aún deben ser compatibles con Virtual Storage Console (VSC).

Limitaciones relacionadas con la gestión de perfiles

- Si actualiza el perfil para separar los backups de los registros de archivos, no se puede realizar una operación de reversión en el host.
- Si activa un perfil desde la GUI para crear copias de seguridad de registros de archivo y después intenta actualizar el perfil mediante la ventana actualización de perfiles múltiples o la ventana actualización de perfiles, no puede modificar dicho perfil para crear una copia de seguridad completa.

- Si actualiza varios perfiles en la ventana actualización de varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** se desactiva.
- Si actualiza varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** de la ventana actualización de perfiles múltiples está desactivada.
- Si cambia el nombre del perfil, no puede revertir el host.

Limitaciones relacionadas con las operaciones de actualización o reversión

- Si intenta instalar una versión anterior de SnapManager para un host sin realizar la operación de reversión en el host en el repositorio, es posible que no pueda realizar lo siguiente:
  - Ver los perfiles que se crearon en versiones anteriores o posteriores de SnapManager para el host.
  - Acceda a los backups o clones que se crearon en las versiones anteriores o posteriores de SnapManager.
  - Realice operaciones de reversión o actualización en el host.
- Después de separar los perfiles para crear backups de registro de archivos, no se puede ejecutar una operación de reversión en el repositorio de host relacionado.

Limitaciones relacionadas con las operaciones de copia de seguridad

- Durante la recuperación, si el backup ya está montado, SnapManager no volverá a montar el backup y utiliza el backup ya montado.

  Si el backup está montado por un usuario diferente y no tiene acceso al backup montado anteriormente, el otro usuario debe proporcionarle el permiso.

  Todos los archivos de registro de archivos tienen permiso de lectura para los usuarios asignados a un grupo; es posible que no tenga el permiso de acceso al archivo de registro de archivos, si el backup se monta por un grupo de usuarios diferente. Los usuarios pueden otorgar permiso a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la operación de restauración o recuperación.

- SnapManager establece el estado de backup como «PROTEGIDO», incluso cuando una de las copias Snapshot del backup de la base de datos se transfiere al sistema de almacenamiento secundario.
- Puede utilizar el archivo de especificación de tareas para la copia de seguridad programada sólo desde SnapManager 3.2 o posterior.
- Si la base de datos del repositorio apunta a más de una dirección IP y cada dirección IP tiene un nombre de host diferente, la operación de programación de backup se realiza correctamente para una dirección IP, pero falla para la otra dirección IP.
- En los entornos ONTAP, SnapManager no admite varios destinos secundarios para un volumen de origen.

Limitaciones relacionadas con las operaciones de restauración

- SnapManager no admite la restauración de backups de bases de datos mediante operaciones de restauración rápida o restauración basada en volúmenes en Windows.

  SnapManager 3.3 muestra un mensaje de error cuando se intenta realizar una operación de restauración rápida desde la interfaz de línea de comandos de SnapManager.

Limitaciones relacionadas con las operaciones de clonación

- SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.
- Si los espacios de tablas temporales se encuentran en una ubicación diferente a la ubicación de los archivos de datos, una operación de clonado crea los espacios de tabla en la ubicación de los archivos de datos.

  Sin embargo, si los espacios de tablas temporales son Oracle Managed Files (OMF) ubicados en una ubicación diferente a la ubicación de los archivos de datos, la operación de clonado no crea los espacios de tablas en la ubicación de los archivos de datos. SnapManager no gestiona los OMF.

- SnapManager no puede clonar una base de datos de RAC si selecciona la opción -resetlogs.

Limitaciones relacionadas con archivos de registro de archivos y copias de seguridad

- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino de área de recuperación flash.
- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino en espera.
- Los backups de registros de archivos se retienen en función de la duración de la retención y la clase de retención por horas predeterminada.

  Cuando la clase de retención de backup de registros de archivos se modifica mediante la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager, la clase de retención modificada no se considera para el backup porque los backups de registros de archivo se retienen en función de la duración de la retención.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, el backup de registros de archivos no incluye los archivos de registro de archivos más antiguos que el archivo de registro de archivos faltante.

  Si falta el archivo de registro de archivos más reciente, la operación de backup del registro de archivos falla.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.
- SnapManager consolida los backups de registros de archivos incluso cuando se eliminan los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados.

Limitaciones relacionadas con el cambio del nombre de host de la base de datos de destino

No se admiten las siguientes operaciones de SnapManager cuando se cambia el nombre de host de la base de datos de destino:

- Cambiar el nombre de host de la base de datos de destino desde la interfaz gráfica de usuario de SnapManager.
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil.
- Al mismo tiempo, se actualizan varios perfiles para un nuevo nombre de host de base de datos de destino.
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager.

Limitaciones relacionadas con la CLI o GUI de SnapManager

- Los comandos de la CLI de SnapManager para la operación de creación de perfiles que se generan desde la interfaz gráfica de usuario de SnapManager no tienen opciones de configuración del historial.

  No se puede utilizar el comando profile create para configurar las opciones de retención del historial desde la interfaz de línea de comandos de SnapManager.

- SnapManager no muestra la GUI en Mozilla Firefox cuando no hay Java Runtime Environment (JRE) disponible en el cliente de Windows.
- SnapManager 3.3 no muestra la GUI de SnapManager en Microsoft Internet Explorer 6 en Windows Server 2008 y Windows 7.
- Al actualizar el nombre de host de la base de datos de destino mediante la interfaz de línea de comandos de SnapManager, si hay una o más sesiones abiertas de la interfaz gráfica de usuario de SnapManager, todas las sesiones abiertas de la interfaz gráfica de usuario de SnapManager no pueden responder.
- Al instalar SnapManager en Windows e iniciar la CLI en UNIX, se muestran las características que no son compatibles con Windows.

Limitaciones relacionadas con SnapMirror y SnapVault

- En algunos casos, no se puede eliminar el último backup asociado con la primera copia Snapshot cuando se ha establecido una relación de SnapVault en el volumen.

  Puede eliminar el backup solo cuando se rompa la relación. Este problema se debe a una restricción de la ONTAP con copias Snapshot base. En una relación de SnapMirror, la copia de Snapshot básica se crea mediante el motor de SnapMirror y, en una relación de SnapVault, la copia de Snapshot base es el backup creado mediante SnapManager. Para cada actualización, la copia snapshot básica señala el backup más reciente creado mediante SnapManager.

Limitaciones relacionadas con las bases de datos en espera de Data Guard

- SnapManager no admite bases de datos lógicas en espera de Data Guard.
- SnapManager no admite bases de datos en espera de Active Data Guard.
- SnapManager no permite realizar backups en línea de bases de datos Data Guard en espera.
- SnapManager no permite backups parciales de bases de datos en espera de Data Guard.
- SnapManager no permite la restauración de bases de datos Data Guard en espera.
- SnapManager no permite eliminar archivos de registro de archivos para bases de datos en espera de Data Guard.
- SnapManager no admite Data Guard Broker.

Información relacionada

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Las funciones de SnapManager y las tecnologías de Oracle no son compatibles con Windows

SnapManager no admite algunas funciones de SnapManager, plataformas ni tecnologías de Oracle en Windows.

SnapManager no admite las siguientes funciones, plataformas y tecnologías de Oracle:

- Protección de datos basada en normativas disponible con la integración de Protection Manager
- Control de acceso basado en roles (RBAC) disponible con Operations Manager
- Restauración rápida o SnapRestore basado en volúmenes (VBSR)
- Operación de división de clones
- Real Application Clusters (RAC) de Oracle utilizando cualquier protocolo
- Oracle Automatic Storage Management (ASM) con cualquier protocolo
- Oracle Direct NFS (dNFS)
- Plataformas Itanium-64

> Las plataformas de hardware admitidas para el sistema operativo Windows son de 32 y 64 bits (Windows x86 y Windows x86_64).

Limitaciones de SnapManager para Clustered Data ONTAP

Debe conocer las limitaciones de algunas funcionalidades y operaciones de SnapManager si utiliza Clustered Data ONTAP.

Las siguientes funcionalidades no son compatibles si utiliza SnapManager en Clustered Data ONTAP:

- Número de unidad lógica (LUN) de asignación de dispositivos sin formato (RDM) para máquinas virtuales de almacenamiento (SVM)
- Una base de datos en la que una LUN pertenece a un sistema que ejecuta Data ONTAP en 7-Mode y la otra LUN pertenece a un sistema que ejecuta Clustered Data ONTAP
- SnapManager para Oracle no admite la migración de un Vserver, que no es compatible con Clustered Data ONTAP
- SnapManager para Oracle no admite la funcionalidad Clustered Data ONTAP 8.2.1 para especificar diferentes políticas de exportación para volúmenes y qtrees

Limitaciones relacionadas con Oracle Database

Antes de empezar a trabajar con SnapManager, debe conocer las limitaciones relacionadas con la base de datos de Oracle.

Estas limitaciones son las siguientes:

- SnapManager es compatible con las versiones 10gR2, 11gR1, 11gR2 y 12*c*_, pero no es compatible con Oracle 10gR1 como repositorio o base de datos de destino.
- SnapManager no admite el uso de una dirección IP DE EXPLORACIÓN en lugar de un nombre de host.

  SCAN IP es una nueva función de Oracle 11gR2.

- SnapManager no es compatible con Oracle Cluster File System (OCFS).
- La compatibilidad con bases de datos Oracle 9i se usa en SnapManager 3.2.
- La compatibilidad con la base de datos Oracle 10gR2 (anterior a 10.2.0.5) queda obsoleta en SnapManager 3.3.1.

Identifique las distintas versiones de las bases de datos de Oracle que se admiten en la matriz de interoperabilidad.

Información relacionada

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Versiones obsoletas de la base de datos Oracle

SnapManager 3.2 o posterior no admite la base de datos Oracle 9i, y la base de datos Oracle 10gR2 (anterior a 10.2.0.4) no es compatible con SnapManager 3.3.1 o posterior.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o posterior, no puede crear perfiles nuevos; se muestra un mensaje de advertencia.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o una versión posterior, debe realizar una de las siguientes acciones:

- Actualice las bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) a bases de datos de Oracle 10gR2 (10.2.0.5), 11gR1 o 11gR2 y, a continuación, actualice a SnapManager 3.2 o 3.3.

  Si va a actualizar a Oracle 12*c*, debe actualizar a SnapManager 3.3.1 o posterior.

  La base de datos Oracle 12*c* sólo se admite desde SnapManager 3.3.1.

- Gestión de las bases de datos Oracle 9i mediante una versión de revisión de SnapManager 3.1.

  Puede utilizar SnapManager 3.2 o 3.3 si desea gestionar bases de datos Oracle 10gR2, 11gR1 o 11gR2 y utilizar SnapManager 3.3.1 o posterior si desea gestionar bases de datos Oracle 12*c* junto con otras bases de datos compatibles.

Instalar SnapManager para Oracle

Puede descargar e instalar SnapManager para Oracle en el entorno y realizar operaciones como backup, restauración, recuperación y clonado de bases de datos.

El paquete de instalación de SnapManager para Oracle incluye el software de servidor host y el software de cliente de la interfaz gráfica de usuario (GUI).

Preparar la instalación de SnapManager para Oracle

El entorno en el que se instala SnapManager para Oracle debe cumplir con determinados requisitos de software, hardware, explorador, base de datos y sistema operativo. Para obtener la información más reciente sobre los requisitos, consulte la matriz de interoperabilidad.

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Tareas de preinstalación

Antes de instalar SnapManager para Oracle, debe realizar algunas tareas adicionales para configurar el entorno. Las tareas que debe realizar dependen del sistema operativo, los componentes de Oracle y la versión de la base de datos que desee utilizar.

- Instalar el sistema operativo con licencia con los parches adecuados.
- Defina los idiomas del sistema operativo y de la base de datos Oracle en inglés.

  Por ejemplo, para establecer el idioma de la base de datos Oracle en inglés ASSIGN NLS_LANG = AMERICAN_AMERICA.WE8MSWIN1252. Para obtener más información acerca de cómo configurar el idioma, consulte la sección *Troubleshooting SnapManager for Oracle*.

- Instale Oracle Recovery Manager (RMAN) si desea utilizar RMAN con SnapManager para Oracle.
- Instalar Data ONTAP con licencias habilitadas para SnapRestore y los protocolos compatibles como Fibre Channel (FC) y Internet Small Computer System Interface (iSCSI) en todos los sistemas de almacenamiento.
- Instale los siguientes parches de Oracle, si utiliza las bases de datos Oracle 11.2.0.2 y 11.2.0.3:
  - 13413167 para Windows de 32 bits
  - 13555974 para Windows de 64 bits

Información relacionada

Resolución de problemas de SnapManager

"Matriz de interoperabilidad de NetApp: support.netapp.com/NOW/products/interoperability"

"Prácticas recomendadas de SnapManager para Oracle: media.netapp.com/documents/tr-3761.pdf"

Descargue el paquete de instalación de SnapManager para Oracle

Puede descargar el paquete de instalación de SnapManager para Oracle en el sitio de soporte de NetApp.

1. Inicie sesión en el sitio de soporte de NetApp.
2. En la página de soporte de NetApp, haga clic en **Descargas** > **Software**.
3. En la tabla Descarga de software, vaya a la fila de productos SnapManager y seleccione **Oracle (Windows)** en la lista desplegable Seleccionar plataforma.
4. Haga clic en **Ir**.

   Se muestra una lista de las versiones de SnapManager.

5. Haga clic en **Ver y descargar** para la versión SnapManager que desea instalar.

   Se muestra la página de descripción.

   Debe leer la información disponible en esta página.

6. En la parte inferior de esta página, haga clic en **continuar**.

Aparecerá la página de acuerdo de licencia.

Debe leer la información disponible en esta página.

7. Haga clic en **Aceptar**.

   Aparece la página de descarga.

8. Descargue el paquete de instalación para el host.

   Puede descargar el archivo de instalación en cualquier ubicación de la máquina en la que desea instalar SnapManager para Oracle.

"Sitio de soporte de NetApp: mysupport.netapp.com"

Instalar SnapManager para Oracle

Puede instalar SnapManager en el host que tenga una o más bases de datos que gestionar. Solo puede instalar una instancia de SnapManager por host.

- Debe haber completado las tareas previas a la instalación necesarias.
- Se debe descargar el paquete de instalación de SnapManager más reciente.
- La versión adecuada de SnapDrive para Windows debe estar instalada y configurada en todos los hosts de destino.

  Para obtener información acerca de la instalación y configuración de SnapDrive para Windows, consulte *SnapDrive for Windows Guía de instalación y administración*.

  a. Haga doble clic en el archivo de instalación de SnapManager:

Si el sistema operativo es…	Utilice…
Windows x86	netapp.smo.windows-x86-version.exe
Windows x64	netapp.smo.windows-x64-version.exe

  Aparece el siguiente mensaje: No se pudo verificar el editor. ¿Está seguro de que desea ejecutar este software?

  b. Haga clic en **Aceptar**.
  c. En la ventana Introducción, haga clic en **Siguiente**.
  d. En la ventana elegir carpeta de instalación, haga clic en **Siguiente** para aceptar la ubicación de instalación predeterminada o seleccione una nueva ubicación.

     La ubicación predeterminada es: C:\Program Files\NetApp\SnapManager para Oracle.

  e. En la ventana disponibilidad de menús, haga clic en **Siguiente**.
  f. En la ventana Specify Service Properties (especificar propiedades del servicio), introduzca la información de cuenta y contraseña para el servicio Windows.

La cuenta especificada debe ser miembro de los siguientes grupos:

- El grupo de administración local del sistema de almacenamiento
- Grupo del administrador local
- El grupo ORA_DBA permite especificar si el servicio debe iniciarse automáticamente después del reinicio o si debe iniciarse manualmente.

g. En la ventana Resumen de preinstalación, haga clic en **instalar**.

h. En la ventana instalar completado, haga clic en **Siguiente**.

i. En la ventana Información importante, haga clic en **hecho** para salir del instalador.

Una vez finalizada la instalación, puede verificar que la instalación se ha realizado correctamente:

1. Inicie el servidor SnapManager:
   a. En la ventana Servicios de Windows, seleccione **NetApp SnapManager version for Oracle**.
   b. En el panel izquierdo, haga clic en **Inicio**.
2. Compruebe que el sistema SnapManager funciona correctamente:
   a. Haga clic en **Inicio** > **programas** > **NetApp** > **SnapManager para Oracle** > **Iniciar la interfaz de línea de comandos (CLI)** de SMO.
   b. En la interfaz de línea de comandos (CLI), introduzca el siguiente comando: Compruebe que el sistema smo muestre el siguiente mensaje: Número de ID de la operación correcto.

   Número es el número de identificación de la operación.

Información relacionada

Preparar la instalación de SnapManager para Oracle

Tareas de preinstalación

Descargue el paquete de instalación de SnapManager para Oracle

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Actualizar SnapManager

Puede realizar una actualización a la versión más reciente de SnapManager para Oracle desde cualquiera de las versiones anteriores. Es posible actualizar todos los hosts SnapManager a la vez o realizar una actualización gradual, lo que permite actualizar los hosts de forma escalonada de host por host.

Preparando la actualización de SnapManager

El entorno en el que desea actualizar SnapManager debe cumplir con los requisitos específicos de software, hardware, explorador, base de datos y sistema operativo. Para obtener la información más reciente sobre los requisitos, consulte la matriz de interoperabilidad.

Antes de la actualización, debe asegurarse de realizar las siguientes tareas:

- Complete las tareas de preinstalación necesarias.
- Descargue el último paquete de instalación de SnapManager para Oracle.
- Instale y configure la versión adecuada de SnapDrive para Windows en todos los hosts de destino.
- Crear un backup de la base de datos del repositorio de SnapManager para Oracle existente.

"Matriz de interoperabilidad: support.netapp.com/NOW/products/interoperability"

Actualizar hosts SnapManager

Es posible actualizar todos los hosts SnapManager existentes para utilizar la versión más reciente de SnapManager. Todos los hosts se actualizan simultáneamente. Sin embargo, esto puede provocar un tiempo de inactividad de todos los hosts SnapManager y las operaciones programadas durante ese tiempo.

1. Detenga el servidor SnapManager siguiendo estos pasos:
   a. En la ventana Servicios de Windows, seleccione **SnapManager de NetApp para Oracle**.
   b. En el panel izquierdo, haga clic en **Detener**.
2. Haga doble clic en el archivo de instalación de SnapManager.

Si el sistema operativo es…	Utilice…
Windows x86	netapp.smo.windows-x86-version_number.exe
Windows x64	netapp.smo.windows-x64-version_number.exe

   Aparece el siguiente mensaje: No se pudo verificar el editor. ¿Está seguro de que desea ejecutar este software?

3. Haga clic en **Aceptar**.

   Aparece la ventana Introducción.

4. Haga clic en **Siguiente**.

   Aparece la ventana elegir carpeta de instalación.

5. Haga clic en **Siguiente** para aceptar la ubicación de instalación predeterminada o seleccionar una nueva ubicación.

   La ubicación predeterminada es: C:\Program Files\NetApp\SnapManager para Oracle.

6. En la ventana disponibilidad de menús, haga clic en **Siguiente**.
7. En la ventana Specify Service Properties (especificar propiedades del servicio), introduzca la información de cuenta y contraseña para el servicio Windows.

   La cuenta especificada debe ser miembro de los siguientes grupos:

- El grupo de administración local del sistema de almacenamiento
- Grupo del administrador local
- El grupo ORA_DBA puede especificar si el servicio debe iniciarse automáticamente después del reinicio o si el servicio debe iniciarse manualmente.

8. En la ventana Resumen de preinstalación, haga clic en **instalar**.
9. En la ventana instalar completado, haga clic en **Siguiente**.
10. En la ventana Información importante, haga clic en **hecho** para salir del instalador.

Información relacionada

Preparar la instalación de SnapManager para Oracle

Tareas de preinstalación

Descargue el paquete de instalación de SnapManager para Oracle

Tareas posteriores a la actualización

Después de actualizar a una versión posterior de SnapManager, es necesario actualizar el repositorio existente. También es posible que desee modificar la clase de retención de backup asignada a los backups existentes.

> Después de actualizar a SnapManager 3.3 o posterior, debe establecer sqlnet.authentication_services a NONE si desea utilizar la autenticación de base de datos (DB) como el único método de autenticación. Esta función no es compatible con las bases de datos RAC.

Actualizando el repositorio existente

No es necesario actualizar el repositorio existente si va a actualizar de SnapManager 3.3.x a SnapManager 3.4 o posterior pero para el resto de las rutas de actualización debe actualizar el repositorio existente para poder acceder a él después de la actualización.

- El servidor SnapManager actualizado debe haberse iniciado y verificado.
- Debe existir un backup del repositorio existente.
- Si va a actualizar desde cualquier versión anterior a SnapManager 3.1 a SnapManager 3.3 o posterior, primero debe actualizar a SnapManager 3.2.

  Después de actualizar a SnapManager 3.2, puede actualizar a SnapManager 3.3 o una versión posterior.

- Después de actualizar el repositorio, no se puede utilizar el repositorio con una versión anterior de SnapManager.
  a. Actualice el repositorio existente: Actualización del repositorio de smo -repository -dbname repository_service_name -host repository_name -login -username Repository_user_name -Port Repository_Port
     - El nombre de usuario del repositorio, el nombre de servicio del repositorio y el nombre de host del repositorio pueden consistir en caracteres alfanuméricos, un signo menos, un guión bajo y un

punto.

- El puerto del repositorio puede ser cualquier número de puerto válido. Las demás opciones utilizadas durante la actualización del repositorio existente son las siguientes:
- La opción de fuerza
- La opción noprompt
- La opción silenciosa
- La opción verbose

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521

+
```

Reinicie el servidor SnapManager para reiniciar todas las programaciones asociadas.

Modificación de la clase de retención de backups

El SnapManager actualizado asigna la clase de retención de backup predeterminada a las copias de seguridad existentes. Puede modificar los valores predeterminados de la clase de retención para cumplir sus requisitos de copia de seguridad.

La clase de retención de copias de seguridad predeterminada asignada a las copias de seguridad existentes es la siguiente:

Tipo de backup	Asignación de clase de retención después de la actualización
Los backups se retienen siempre	Ilimitada
Otros backups	Todos los días

Nota: puede eliminar las copias de seguridad que se conservan para siempre sin cambiar la clase de retención.

Si actualiza a SnapManager 3.0 o posterior, el valor mayor de los siguientes dos valores se asignará a los perfiles existentes:

- Recuento de retención anterior para el perfil
- Valores predeterminados para el recuento de retención y la duración de los backups diarios, como se especifica en el archivo smo.config
  a. Modifique los valores asignados a retain.Hourly.count y Retain.Hourly.Duration en el archivo smo.config.

     Puede introducir los siguientes valores:

     - retain.hourly.count = 12
     - retain.hourly.duration = 2

Información relacionada

Parámetros de configuración de SnapManager

Actualizar hosts de SnapManager mediante actualización gradual

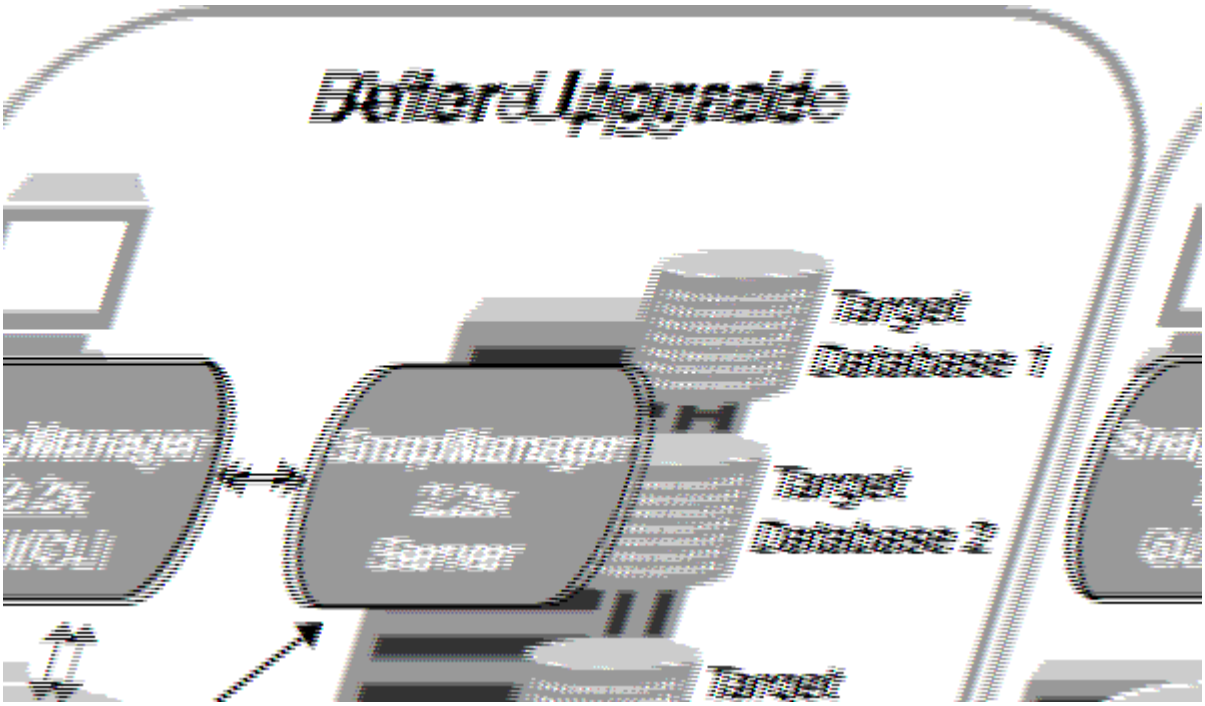
El enfoque de actualización gradual que permite actualizar los hosts de forma escalonada y host por host se admite desde SnapManager 3.1.

SnapManager 3.0 o versiones anteriores solo permitió actualizar todos los hosts al mismo tiempo. Esto provocó un tiempo de inactividad de todos los hosts SnapManager y las operaciones programadas durante la operación de actualización.

La actualización gradual ofrece las siguientes ventajas:

- Se ha mejorado el rendimiento de SnapManager porque solo se actualiza un host a la vez.
- Capacidad para probar las nuevas funciones en un host de servidor SnapManager antes de actualizar los otros hosts.

Solo se puede realizar la actualización gradual mediante la interfaz de línea de comandos (CLI).



Después de completar correctamente la actualización, los hosts de SnapManager, los perfiles, las programaciones, las backups, Además, los clones asociados con los perfiles de las bases de datos de destino se migran de la base de datos del repositorio de la versión de SnapManager anterior a la base de datos del repositorio de la nueva versión. Los detalles sobre las operaciones realizadas mediante los perfiles, las programaciones, los backups y los clones que se crearon con la versión anterior de SnapManager ahora están disponibles en la base de datos del repositorio de la nueva versión. Puede iniciar la GUI utilizando los valores de configuración predeterminados del archivo user.config. No se consideran los valores configurados en el archivo user.config de la versión anterior de SnapManager.

El servidor SnapManager actualizado ahora puede comunicarse con la base de datos del repositorio actualizada. Los hosts que no se actualizaron pueden gestionar sus bases de datos de destino mediante el

repositorio de la versión anterior de SnapManager y, por lo tanto, pueden utilizar las funciones disponibles en la versión anterior.

> Antes de realizar la actualización gradual, debe asegurarse de que todos los hosts de la base de datos del repositorio puedan resolverse. Para obtener información acerca de cómo resolver los hosts, consulte la sección de solución de problemas en *SnapManager for Oracle Administration Guide for UNIX*.

Información relacionada

Qué es una reversión

Resolución de problemas de SnapManager

Requisitos previos para realizar la actualización gradual

Antes de realizar una actualización gradual, debe asegurarse de que el entorno cumpla ciertos requisitos.

- Si utiliza cualquier versión anterior a SnapManager 3.1 y desea realizar una actualización gradual a SnapManager 3.3 o posterior, primero debe actualizar a la versión 3.2 y, después, a la última.

  Puede actualizar directamente de SnapManager 3.2 a SnapManager 3.3 o posterior.

- Deben realizarse backups de los scripts externos que se usan para realizar cualquier protección de datos externa o retención de datos.
- Debe instalarse la versión de SnapManager a la que desea actualizar.

  > Si va a actualizar desde cualquier versión anterior a SnapManager 3.1 a SnapManager 3.3 o posterior, primero debe instalar SnapManager 3.2 y realizar una actualización gradual. Después de actualizar a la versión 3.2, puede instalar SnapManager 3.3 o posterior y realizar otra actualización gradual a SnapManager 3.3 o posterior.

- Debe instalarse la versión de SnapDrive para Windows compatible con la versión de SnapManager a la que desea actualizar.

  Para obtener información sobre la instalación de SnapDrive, consulte el conjunto de documentación de SnapDrive.

- Debe realizarse un backup de la base de datos del repositorio.
- La cantidad de utilización de repositorio de SnapManager debe ser mínima.
- Si el host que se va a actualizar utiliza un repositorio, no deben realizarse operaciones de SnapManager en los demás hosts que utilizan el mismo repositorio.

  Las operaciones que están programadas o en ejecución en los otros hosts esperarán a que se complete la actualización gradual.

- Los perfiles que apuntan a la misma base de datos de repositorio deben crearse con nombres diferentes en los hosts de servidor SnapManager.

  Si utiliza perfiles con el mismo nombre, la actualización gradual que implica esa base de datos del repositorio falla sin previo aviso.

- No deben realizarse operaciones de SnapManager en el host que se está actualizando.

> La actualización gradual se ejecuta durante más tiempo a medida que aumenta el número de backups de los hosts que se van actualizando conjuntamente. La duración de la actualización puede variar según la cantidad de perfiles y backups asociados con un host determinado.

Información relacionada

Instalar SnapManager para Oracle

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Realizar la actualización gradual en un único host o en varios hosts

Puede realizar la actualización gradual en un único o varios hosts de servidor SnapManager mediante la interfaz de línea de comandos (CLI). El host del servidor SnapManager actualizado se gestiona únicamente con la versión posterior de SnapManager.

Debe asegurarse de que se hayan completado todos los requisitos previos para realizar la actualización gradual.

1. Para realizar una actualización sucesiva en un solo host, introduzca el siguiente comando: Smorepostory rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-upgrade-hoshost_with_target_database-force [-quiet | -verbose]

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino montadas en Hosta y una base de datos de repositorio denominada REPOA ubicada en repo_host:

   ```
   smo repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA
   ```

2. Para realizar una actualización sucesiva en varios hosts, introduzca el siguiente comando: Smorepostory rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-upgrade-hostist_with_target_database1,host_with_target_target_fle2 | verbose [-verbose]

   > En el caso de varios hosts, introduzca los nombres de hosts separados por una coma y asegúrese de no incluir espacio entre la coma y el siguiente nombre de host.Además, asegúrese de introducir todos los nombres de hosts entre comillas dobles.

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino montadas en los hosts, Hosta y HostB y una base de datos de repositorio denominada REPOA ubicada en repo_host:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -upgradehost hostA,hostB
```

3. Para realizar una actualización sucesiva en todos los hosts de una base de datos de repositorio, introduzca el siguiente comando: Smorepipository rollingupgrade-repository-dbnamerepo_service_name-strepo_host-login-usernamerepo_username-portrepo_Port-allhosts-force [-quiet | -verbose]

   Después de actualizar correctamente la base de datos de repositorio, puede realizar todas las operaciones de SnapManager en la base de datos de destino.

   La actualización de SnapManager para Oracle conserva las credenciales de usuario basadas en host, las credenciales de usuario del software de Oracle y las credenciales de usuario de Oracle Recovery Manager (RMAN) desde la versión anterior de SnapManager para Oracle.

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino disponibles en una base de datos de repositorio denominada REPOA ubicada en repo_host:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
      -allhosts
```

   - Si el servidor SnapManager se inicia automáticamente, debe reiniciar el servidor para garantizar que pueda ver las programaciones.
   - Si actualiza uno de los dos hosts relacionados, debe actualizar el segundo host después de actualizar el primero.

     Por ejemplo, si ha creado un clon del host A al host B o montado un backup del host A al host B, los hosts A y B están relacionados entre sí. Cuando se actualiza el host A, aparece un mensaje de advertencia en el que se le solicita actualizar el host B poco después de actualizar el host A.

     > Los mensajes de advertencia se muestran aunque el clon se elimina o el backup se desasocia del host B durante la actualización gradual del host A. Esto se debe a que existen metadatos en el repositorio para las operaciones realizadas en el host remoto.

Información relacionada

Requisitos previos para realizar la actualización gradual

Qué es una reversión

La operación de reversión permite revertir a una versión anterior de SnapManager después de realizar una actualización gradual.

> Antes de realizar una reversión, debe asegurarse de que todos los hosts en la base de datos del repositorio puedan resolverse.

Al realizar una reversión, se revierte lo siguiente:

- Los backups creados, liberados y eliminados mediante la versión de SnapManager desde la que se está revirtiendo
- Los clones creados a partir de un backup que se creó mediante la versión de SnapManager a partir de la cual se va a revertir
- Las credenciales de perfil modificadas por medio de la versión de SnapManager de la que se va a revertir

No se admiten las funciones disponibles en la versión de SnapManager que utilizaba, pero no están disponibles en la versión en la que se está revirtiendo. Por ejemplo, cuando realiza una reversión desde SnapManager 3.3 o posterior a SnapManager 3.1, la configuración de historial establecida para perfiles en SnapManager 3.3 o posterior no se revierte a los perfiles en SnapManager 3.1. Esto se debe a que la característica de configuración del historial no estaba disponible en SnapManager 3.1.

Información relacionada

Resolución de problemas de SnapManager

Limitaciones en la ejecución de una reversión

Debe conocer cuáles son las situaciones en las que no se puede ejecutar una reversión. No obstante, en algunas de estas situaciones es posible ejecutar algunas tareas adicionales antes de realizar la reversión.

Los casos en los que no se puede ejecutar la reversión o se debe realizar las tareas adicionales son los siguientes:

- Si realiza una de las siguientes operaciones después de realizar una actualización gradual:
  - Cree un nuevo perfil.
  - Cambie el estado de montaje del backup.

    En este caso, primero debe cambiar el estado de montaje a su estado original y, a continuación, ejecutar una reversión.

  - Restaurar un backup.
  - Cambie el modo de autenticación de la autenticación de la base de datos a la autenticación del sistema operativo (SO).

    En esta situación, después de realizar una reversión, debe cambiar manualmente el modo de autenticación de sistema operativo a base de datos.

- Si se cambia el nombre de host del perfil
- Si se separan perfiles para crear backups de registros de archivo

  En este caso, no puede volver a una versión anterior a SnapManager 3.2.

Requisitos previos para ejecutar una reversión

Antes de realizar una reversión, debe asegurarse de que el entorno cumpla con ciertos requisitos.

- Si utiliza SnapManager 3.3 o una versión posterior y desea revertir a una versión anterior a SnapManager 3.1, tendrá que volver a la versión 3.2 y, a continuación, a la versión deseada.
- Deben realizarse backups de los scripts externos que se usan para realizar cualquier protección de datos externa o retención de datos.
- Debe instalarse la versión de SnapManager a la que desea revertir.

  > Si desea realizar una reversión de SnapManager 3.3 o posterior a una versión anterior a SnapManager 3.1, primero debe instalar SnapManager 3.2 y realizar una reversión. Después de revertir a 3.2, puede instalar SnapManager 3.1 o una versión anterior y realizar otra reversión a esa versión.

- Debe instalarse la versión de SnapDrive para Windows compatible con la versión de SnapManager a la que desea revertir.

  Para obtener información sobre la instalación de SnapDrive, consulte el conjunto de documentación de SnapDrive.

- Debe realizarse un backup de la base de datos del repositorio.
- Si el host que se va a revertir utiliza un repositorio, no debe realizarse operaciones de SnapManager en los demás hosts que utilizan el mismo repositorio.

  Las operaciones que están programadas o en ejecución en los otros hosts esperan a que se complete la reversión.

- Los perfiles que apuntan a la misma base de datos del repositorio deben crearse con nombres diferentes en los hosts del servidor SnapManager.

  Si se utilizan perfiles con el mismo nombre, la operación de reversión que implica la base de datos del repositorio generará un error sin previo aviso.

- No se deben realizar operaciones de SnapManager en el host al que se desea revertir.

  Si existe una operación en ejecución, debe esperar hasta que se complete esa operación y antes de continuar con la reversión.

> La operación de reversión se ejecuta durante más tiempo a medida que aumenta la cantidad acumulativa de backups de los hosts que se están revertir juntos. La duración de la reversión puede variar según la cantidad de perfiles y backups asociados con un host determinado.

Información relacionada

Instalar SnapManager para Oracle

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Ejecución de una reversión en un solo host o varios hosts

Puede realizar una reversión en una sola o varios hosts de servidor SnapManager con la interfaz de línea de comandos (CLI).

Se debe asegurarse de que se hayan completado todos los requisitos previos para realizar una reversión.

1. Para realizar una reversión en un solo host, escriba el siguiente comando: Smorepostory rollback-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-rollbackhosthost_with_target_database

   En el ejemplo siguiente se muestra el comando para revertir todas las bases de datos de destino montadas en Hosta y una base de datos de repositorio denominada REPOA ubicada en el host de repositorio, repo_host:

   ```
   smo repository rollback
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -rollbackhost hostA
   ```

2. Para realizar una reversión en varios hosts, introduzca el siguiente comando: Smorepostory rollback-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_Port-rollbackhoshost_with_target_database1,host_with_target_target_database2

   > Para varios hosts, introduzca los nombres de host separados por una coma y asegúrese de que no haya espacio entre la coma y el siguiente nombre de host.Además, asegúrese de introducir todo el conjunto de varios nombres de host entre comillas dobles.

   En el ejemplo siguiente se muestra el comando para revertir todas las bases de datos de destino montadas en los hosts, Hosta, HostB y una base de datos de repositorio denominada REPOA ubicada en el host de repositorios, repo_host:

   ```
   smo repository rollback
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -rollbackhost hostA,hostB
   ```

Los hosts, los perfiles, las programaciones, los backups y los clones que están asociados con los perfiles de las bases de datos de destino para el host se revierten al repositorio anterior.

Información relacionada

Requisitos previos para ejecutar una reversión

Tareas posteriores a la reversión

Es necesario realizar algunos pasos adicionales después de revertir una base de datos de repositorio y degradar el host de SnapManager de SnapManager 3.2 a SnapManager 3.0, para ver las programaciones creadas en la versión anterior de la base de datos del repositorio.

1. Desplácese hasta C:\Program Files\NetApp\SnapManager para Oracle\repositories.

   El directorio de repositorios puede contener dos archivos para cada repositorio. El nombre de archivo con el signo de número (#) se crea utilizando SnapManager 3.1 o posterior y el nombre de archivo con el guión (-) se crea utilizando SnapManager 3.0.

   Los nombres de los archivos pueden ser los siguientes:

   - Repository#SMO300a#SMOREPO1#10.72.197.141#1521
   - repository-smo300a-smorepo1-10.72.197.141-1521
2. Reemplace el signo de número (#) en el nombre de archivo por el guión (-).

   El nombre de archivo que tenía el signo de número (#) contiene ahora guión (-): Repository-SMO300a-SMOREPO1-10.72.197.141-1521.

Configurando SnapManager

Después de instalar SnapManager, debe realizar algunas tareas de configuración adicionales según el entorno que utilice.

Parámetros de configuración de SnapManager

SnapManager proporciona una lista de parámetros de configuración que se pueden editar en función de sus requisitos. Los parámetros de configuración se almacenan en el archivo smo.config. Sin embargo, es posible que el archivo smo.config no contenga todos los parámetros de configuración admitidos. Puede agregar los parámetros de configuración, según sus necesidades.

En la siguiente tabla, se enumeran todos los parámetros de configuración de SnapManager compatibles y también se explica cuándo usar estos parámetros:

Parámetros	Descripción

• retain.hourly.count • retain.hourly.duration • retenga.monthly.count • retain.monthly.duration	Estos parámetros configuran la política de retención al crear un perfil. Por ejemplo, puede asignar los siguientes valores:retain.Hourly.count = 12 retain.hourly.duration = 2 retenga.monthly.count = 2 retain.monthly.duration = 6
Restore.temporaryVolumeName	Este parámetro asigna un nombre al volumen temporal. Cuando SnapManager utiliza el método indirecto para restaurar datos desde el almacenamiento secundario, requiere un volumen de desecho en el almacenamiento principal para conservar una copia temporal de los datos hasta que se copian en los archivos de la base de datos y se recupera la base de datos. No hay un valor predeterminado. Si no especifica un valor, debe introducir un nombre en el comando restore que utilice el método indirecto. Por ejemplo, puede asignar los siguientes valores:restore.temporaryVolumeName = smo_temp_volume
host.credenciales.persistir	Este parámetro permite que SnapManager almacene credenciales del host. De manera predeterminada, las credenciales del host no se almacenan. Sin embargo, se deben almacenar las credenciales de host si tiene un script personalizado que se ejecuta en un clon remoto y requiere acceso a un servidor remoto. Para habilitar el almacenamiento de credenciales de host, asigne TRUE al host.credenciales.persistir. SnapManager cifra y guarda las credenciales del host.
RestorePlanMaxFilesDisjugado	Este parámetro permite definir el número máximo de archivos que se mostrarán en la vista previa de la restauración.de forma predeterminada, SnapManager muestra un máximo de 20 archivos en la vista previa de la restauración. Sin embargo, puede cambiar a un valor mayor que 0. Por ejemplo, puede asignar el siguiente valor: • RestorePlanMaxFilesDisjugado = 30 Si especifica un valor no válido, se muestra el número predeterminado de archivos.

snapshot.list.timeout.min	Este parámetro permite definir el tiempo en minutos durante el cual SnapManager debe esperar a que se ejecute el comando snap list al realizar cualquier operación de SnapManager.de forma predeterminada, SnapManager espera 30 minutos. Sin embargo, puede cambiar a un valor mayor que 0. Por ejemplo, puede asignar el siguiente valor: • snapshot.list.timeout.min = 40 Si especifica un valor no válido, se utiliza el valor predeterminado. Para cualquier operación de SnapManager, si el tiempo de ejecución del comando snap list supera el valor asignado a snapshot.list.timeout.min, la operación genera un mensaje de error de tiempo de espera.
PruneIfFileExistsInOtherDestination	Este parámetro de eliminación permite definir el destino de los archivos de registros de archivos. Los archivos de registro de archivos se almacenan en varios destinos. Al eliminar los archivos de registro de archivos, SnapManager debe conocer el destino de los archivos de registro de archivos. Los posibles valores que puede asignar son los siguientes: • Cuando desee quitar los archivos de registro de archivo de un destino especificado, debe asignar false a pruneIfFileExistsInOtherDestination. • Cuando desee quitar los archivos de registro de archivo de un destino externo, debe asignar true a pruneIfFileExistsInOtherDestination.

prune.archivelogs.backedup.from.otherdestination	Este parámetro de eliminación permite reducir los archivos de registro de archivos de los que se ha realizado una copia de seguridad desde los destinos de registro de archivos especificados o del que se ha realizado una copia de seguridad desde destinos de registros de archivos externos. Los posibles valores que puede asignar son los siguientes: • Si desea comprimir los archivos de registro de archivos desde los destinos especificados y si se realiza un backup de los archivos de registro de archivos desde los destinos especificados mediante -prune-dest, debe asignar false a prune.archivelogs.backedup.from.otherdestination . • Si desea comprimir los archivos de registro de archivos desde destinos especificados y si se realiza una copia de seguridad de los archivos de registro de archivos al menos una vez desde cualquiera de los otros destinos, debe asignar true a prune.archivelogs.backedup.from.otherdestination .
Maximum.archivvelog.files.torune.atATime	Este parámetro de eliminación permite definir el número máximo de archivos de registro de archivos que puede recortar en un momento dado. Por ejemplo, puede asignar el siguiente valor:Maximum.archivvelog.files.torune.atATime = 998 El valor que se puede asignar a Maximum.archivvelog.files.torune.atATime debe ser inferior a 1000.
archvelogs.consolidate	Este parámetro permite a SnapManager liberar las copias de seguridad duplicadas de registros de archivo si asigna true a archivvelogs.consolidate.
suffix.backup.label.with.logs	Este parámetro permite especificar el sufijo que se desea añadir para diferenciar los nombres de etiqueta del backup de datos y del backup de registros de archivo.por ejemplo, al asignar registros al sufijo.backup.label.with.logs, se añade _logs como sufijo a la etiqueta de backup de registros de archivo. La etiqueta de backup del registro de archivos debería ser arch_logs.

backup.archivelogs.beyond.missingfiles	Este parámetro permite que SnapManager incluya los archivos de registro de archivos faltantes en el backup. Los archivos de registro de archivos que no existen en el sistema de archivos activo no se incluyen en la copia de seguridad. Si desea incluir todos los archivos de registro de archivos, incluso los que no existen en el sistema de archivos activo, debe asignar true a backup.archivelogs.beyond.missingfiles. Puede asignar false para ignorar los archivos de registro de archivos que faltan.
srvctl.timeout	Este parámetro permite definir el valor de tiempo de espera para el comando srvctl. **Nota:** el control de servidor (SRVCTL) es una utilidad para administrar instancias de RAC. Cuando SnapManager tarda más tiempo en ejecutar el comando srvctl que el valor timeout, la operación SnapManager produce un error con este mensaje de error: Error: Se ha agotado el tiempo de espera mientras se ejecuta el comando: Srvctl status.
Snapshot.restore.storageNameCheck	Este parámetro permite a SnapManager ejecutar la operación de restauración con copias de Snapshot que se crearon antes de migrar desde operaciones de Data ONTAP en 7-Mode a Clustered Data ONTAP.el valor predeterminado asignado al parámetro es FALSE. Si ha realizado la migración desde Data ONTAP funcionando en 7-Mode a Clustered Data ONTAP, pero quiere utilizar las copias Snapshot creadas antes de la migración, establezca snapshot.restore.storageNameCheck=true.
services.common.disableAbort	Este parámetro deshabilita la limpieza tras el fallo de las operaciones de ejecución prolongada. Puede establecer un ejemplo services.common.disableAbort=true.For, si está realizando una operación de clonado que se ejecuta mucho y, a continuación, se produce un error debido a un error de Oracle, es posible que no desee limpiar el clon. Si establece services.common.disableAbort=true, no se eliminará el clon. Puede corregir el problema de Oracle y reiniciar la operación de clonado desde el punto en que falló.

• backup.sleep.dnfs.layout • backup.sleep.dnfs.secs	Estos parámetros activan el mecanismo de suspensión en el diseño Direct NFS (dNFS). Después de crear la copia de seguridad de los archivos de control con dNFS o un sistema de archivos de red (NFS), SnapManager intenta leer los archivos de control, pero es posible que no se encuentren los archivos.para habilitar el mecanismo de suspensión, asegúrese de que backup.sleep.dnfs.Layout=true. El valor predeterminado es TRUE. Al activar el mecanismo de suspensión, debe asignar el tiempo de suspensión a backup.sleep.dnfs.secs. El tiempo de inactividad asignado es en segundos y el valor depende de su entorno. El valor predeterminado es 5 segundos. Por ejemplo: • backup.sleep.dnfs.layout=true • backup.sleep.dnfs.secs=2
• override.default.backup.pattern • new.default.backup.pattern	Cuando no se especifica la etiqueta de backup, SnapManager crea una etiqueta de backup predeterminada. Estos parámetros de SnapManager permiten personalizar la etiqueta de copia de seguridad predeterminada.para personalizar la etiqueta de copia de seguridad, asegúrese de que el valor de override.default.backup.pattern se establece en true. El valor predeterminado es FALSE. Para asignar el nuevo patrón de la etiqueta de backup, se pueden asignar palabras clave como el nombre de la base de datos, el nombre del perfil, el ámbito, el modo y el nombre del host a new.default.backup.pattern. Las palabras clave se deben separar con un guión bajo. Por ejemplo, new.default.backup.pattern=dbname_profile_hostname_scope_mode. La Marca de hora se incluye automáticamente al final de la etiqueta generada.

allow.underscore.in.clone.sid	Oracle admite el uso de guion bajo en el SID de clonado de Oracle 11gR2. Este parámetro SnapManager permite incluir un guión bajo en el nombre del SID del clon.para incluir un guión bajo en el nombre del SID del clon, asegúrese de que el valor de allow.underscore.in.clone.sid se configure en TRUE. El valor predeterminado es TRUE. Si utiliza una versión de Oracle anterior a Oracle 11gR2 o si no desea incluir un guión bajo en el nombre del SID del clon, establezca el valor en FALSE.
oracle.parameters.with.comma	Este parámetro permite especificar todos los parámetros de Oracle que tienen coma (,) como valor.mientras se realiza cualquier operación, SnapManager usa oracle.parameters.with.comma para comprobar todos los parámetros de Oracle y omitir la división de los valores. Por ejemplo, si el valor de nls_numeric_characters=, especifique oracle.parameters.with.comma=nls_numeric_characters. Si hay varios parámetros de Oracle con coma como valor, debe especificar todos los parámetros en oracle.parameters.with.comma.

• ArchivedLogs.Exclude • ArchivedLogs.exclude.fileslike • <db-unique-name>.archivedLogs.exclude.fileslike	Estos parámetros permiten a SnapManager excluir los archivos de registro de archivado de los perfiles y las copias de seguridad si la base de datos no está en un sistema de almacenamiento habilitado para la copia snapshot y desea realizar operaciones SnapManager en ese sistema de almacenamiento.**Nota:** debe incluir los parámetros de exclusión en el archivo de configuración antes de crear un perfil. Los valores asignados a estos parámetros pueden ser un directorio de nivel superior o un punto de montaje donde están presentes los archivos de registro de archivos o un subdirectorio. Para excluir los archivos de registro de archivos de que se incluyan en el perfil y se realice una copia de seguridad, debe incluir uno de los parámetros siguientes: • ArchivedLogs.exclude para especificar una expresión regular para excluir los archivos de registro de archivos de todos los perfiles o copias de seguridad. Los archivos de registro de archivos que coinciden con la expresión regular se excluyen de todos los perfiles y copias de seguridad. Por ejemplo, puede establecer archivedLogs.Exclude = J:\\ARCH\\.*. Si el destino tiene un separador de archivos, se debe agregar un símbolo de barra diagonal adicional (\) al patrón y éste debe terminar con un patrón de doble barra (\\.*). • ArchivedLogs.exclude.filesLike de especificar una expresión SQL para excluir los archivos de registro de archivos de todos los perfiles o copias de seguridad. Los archivos de registro de archivos que coinciden con la expresión SQL se excluyen de todos los perfiles y las copias de seguridad. Por ejemplo, puede establecer archivedLogs.exclude.fileslike = J:\\ARCH2\\\%. Si el destino tiene un separador de archivos, se debe agregar un símbolo de barra diagonal adicional (\) al patrón y éste debe terminar con un patrón de doble barra (\\%).

	• <db-unique-name>.ArchivedLogs.exclude.filesLike para especificar una expresión SQL para excluir los archivos de registro de archivos sólo del perfil o la copia de seguridad creada para la base de datos con el nombre-único-dB especificado. Los archivos de registro de archivos que coinciden con la expresión SQL se excluyen del perfil y las copias de seguridad. Por ejemplo, puede establecer mydB.archivedLogs.exclude.fileslike = J:\\ARCH2\\%. Si el destino tiene un separador de archivos, se debe agregar un símbolo de barra diagonal adicional (\) al patrón y éste debe terminar con un patrón de doble barra (\\%).

Edición de los parámetros de configuración

Según el entorno, puede cambiar los valores predeterminados asignados al parámetro de configuración.

1. Abra el archivo de configuración desde la siguiente ubicación predeterminada:

   ubicación predeterminada de la instalación\properties\smo.config

2. Cambie los valores predeterminados de los parámetros de configuración.

   También puede agregar parámetros de configuración compatibles que no se incluyen en el archivo de configuración y asignarles valores.

3. Reinicie el servidor de SnapManager para Oracle.

Comenzando por Oracle

La sección de inicio de SnapManager enumera las tareas que se realizan al iniciar SnapManager. Use esta sección también si está aprendiendo acerca de SnapManager.

Antes de usar SnapManager, debe haber realizado las siguientes acciones:

- Se ha descargado e instalado el software de SnapManager.
- Se determinó si utilizará la interfaz gráfica de usuario o la interfaz de línea de comandos.

Identificación de una base de datos existente para realizar una copia de seguridad

Puede identificar el identificador de sistema (SID) de la base de datos de SnapManager que se utiliza para crear un perfil.

El ID de usuario estándar de Oracle para sistemas que no son SAP es oracle.

1. Haga clic en **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. Verifique el servicio Oracle, OracleServiceSID.

   Si el servicio se denomina OracleServiceFASDB, el SID de la base de datos es FASDB.

Verificación del estado del listener de Oracle

Puede verificar el estado del listener de Oracle mediante el comando lsnrctl status.

- Debe conectarse a la base de datos.

Una instalación estándar de Oracle establece el puerto de escucha de la base de datos en 1521.

1. En el símbolo del sistema, introduzca el comando:lsnrctl status

Crear usuarios de Oracle para la base de datos del repositorio

Es posible crear un usuario de Oracle para la base de datos del repositorio y asignar privilegios específicos para ejecutar distintas operaciones en la base de datos del repositorio.

Debe asignar los privilegios de conexión y recursos al usuario de Oracle. No es necesario crear un usuario para la base de datos del repositorio con privilegios de sysdba.

> Sin embargo, debe crear un usuario de Oracle con el rol sysdba para la base de datos de destino.

1. Inicie sesión en SQL *Plus.

   En el símbolo del sistema, escriba el siguiente comando: 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. Para crear un usuario, por ejemplo repo1_user, para el repositorio con la contraseña de administrador, por ejemplo, adminpw1, escriba el siguiente comando en el símbolo del sistema SQL: SQL> create user repo1_user identificado por adminpw1;

3. Para otorgar privilegios de conexión y recursos al usuario, escriba el siguiente comando: Grant connect, resource to repo1_user;

Crear un usuario de Oracle para la base de datos de destino

Debe crear un usuario de Oracle con el rol sysdba que se conecta a la base de datos y realiza operaciones de base de datos.

SnapManager puede utilizar cualquier usuario de Oracle con privilegios sysdba que exista en la base de datos de destino, por ejemplo, el usuario predeterminado "sys". También puede crear un usuario en la base de datos de destino para que la utilice exclusivamente SnapManager.

1. Inicie sesión en SQL *Plus.

   En el símbolo del sistema, escriba el siguiente comando: Sqlplus '/ as sysdba'

2. Para crear un usuario, por ejemplo smo_oper con la contraseña de administrador, por ejemplo, adminpw1, escriba el siguiente comando en el símbolo del sistema SQL: SQL> create user smo_oper identificado por adminpw1;
3. Conceda privilegios de sysdba al usuario de Oracle introduciendo el siguiente comando: SQL> Grant sysdba a smo_oper;

Acceso a SnapManager

Es posible acceder a SnapManager por medio de la interfaz de línea de comandos (CLI) o de la interfaz gráfica de usuario (GUI).

Es posible realizar operaciones de SnapManager distintas de las siguientes maneras:

- Si se introducen comandos en la CLI en un host que está en la misma red que el host de la base de datos.

  Para obtener una lista de todos los comandos y una explicación de sus opciones y argumentos, consulte el capítulo referencia de comandos.

  Para acceder a la CLI, haga clic en **Inicio** > **todos los programas** > **NetApp** > **SnapManager para Oracle** > **Iniciar la interfaz de línea de comandos (CLI)** de SMO.

- Mediante el acceso a la GUI en un host en la misma red que el host de la base de datos.

  La interfaz gráfica de usuario proporciona sencillos asistentes que ayudan a realizar diferentes operaciones.

Información relacionada

Referencia de comandos de SnapManager para Oracle

Iniciar el servidor host SnapManager

Puede iniciar el servidor SnapManager mediante los servicios de Windows.

1. Haga clic en **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. En la ventana Services, seleccione NetAppSnapManager 3.3 para Oracle.

3. Puede iniciar el servidor de una de estas tres formas:
    - En el panel izquierdo, haga clic en **Inicio**.
    - Haga clic con el botón derecho en NetAppSnapManager 3.3 para Oracle y seleccione **Iniciar** en el menú desplegable.
    - Haga doble clic en NetAppSnapManager 3.3 para Oracle y, a continuación, en la ventana Propiedades, haga clic en **Inicio**.

Verificación del estado del servidor host SnapManager

El servidor debe estar en ejecución para que pueda ejecutar comandos o iniciar operaciones de SnapManager. Debe verificar el estado del servidor antes de realizar cualquier operación.

1. En la ventana Servicios, seleccione SnapManager 3.3 para Oracle.
2. Vea el estado en la columna Status.

El uso de comandos de la SnapManager

Después de iniciar el servidor de host SnapManager, puede utilizar SnapManager introduciendo comandos en el símbolo del sistema de su host.

1. Para realizar una operación:
    - En el caso de un host de Windows, vaya a **Inicio** > **todos los programas** > **NetApp** > **SnapManager para Oracle** > **Iniciar la interfaz de línea de comandos (CLI)** de SMO

Inicia la interfaz gráfica de usuario de SnapManager

Si SnapManager está instalado en el host, inicie la interfaz gráfica de usuario (GUI) para SnapManager seleccionando el programa en una lista de programas.

- Asegúrese de que el servidor SnapManager se ha iniciado.

Puede iniciar la interfaz gráfica de usuario de SnapManager de una de las siguientes maneras:

- En el host de SnapManager, haga clic en **Inicio** > **todos los programas** > **NetApp** > **SnapManager para Oracle** > **Iniciar la GUI de SMO**.
- Si SnapManager no está instalado en el host, utilice Java Web Start, que descarga los componentes de SnapManager e inicia la GUI.

Información relacionada

Descarga e inicio de la interfaz gráfica de usuario mediante Java Web Start

Descarga e inicio de la interfaz gráfica de usuario mediante Java Web Start

Es posible utilizar Java Web Start si SnapManager no está instalado en el host. Java Web Start descarga los componentes de SnapManager e inicia la interfaz gráfica de usuario (GUI). Las versiones de JRE compatibles son 1.5, 1.6, 1.7 y 1.8.

Debe asegurarse de que se cumplan las siguientes condiciones:

- El servidor SnapManager se está ejecutando.
- Se abre una ventana del navegador Web.

a. En la ventana del explorador Web de Microsoft Internet Explorer, introduzca https://smo-server.domain.com:port.

   smo-server.domain.com es el nombre de host y dominio completos en los que ha instalado SnapManager y Port es el puerto de escucha del servidor SnapManager (27214, de forma predeterminada).

   > Debe introducir https en la ventana del navegador.

   Un cuadro de diálogo con el mensaje hay un problema con el certificado de seguridad del sitio… ¿desea continuar? aparece en pantalla.

b. Haga clic en **Sí** o **continuar**.

c. Haga clic en el enlace con la etiqueta haga clic aquí para descargar e instalar JRE 6.0 y la aplicación.

   Un vínculo denominado Descargar Java Web Start con el mensaje este sitio podría requerir el siguiente control ActiveX: Java Plug-in 1.6"… "Haga clic aquí para instalar.

d. En la ventana instalar, realice los siguientes pasos:

   i. Haga clic en el mensaje etiquetado haga clic aquí para instalar….

      Aparece el menú **Install ActiveX Control** (instalar control ActiveX*).

   ii. Seleccione **instalar control ActiveX…**.

      El mensaje Internet Explorer - Advertencia de seguridad" que contiene el texto siguiente: "¿desea instalar este software? Nombre: Se muestra Java Plug-in 1.6.

   iii. Haga clic en **instalar**.

      Un "Java Plug-in 1.6". Aparece la ventana del instalador de J2SE Runtime Environment 1.6.

   iv. Haga clic en **instalar**.

   Aparecerá una ventana en la que se le solicitará que instale J2SE Runtime Environment 1.6.

e. En la ventana instalar, realice los siguientes pasos:

   i. En la página Contrato de licencia, seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.

   ii. En la página Tipo de instalación, seleccione **típica** y haga clic en **Siguiente**.

   iii. En la ventana instalación completada, haga clic en **Finalizar**.

      SnapManager comienza la descarga.

   Un cuadro de diálogo Descarga de archivo con el mensaje ¿desea guardar este archivo? se muestra application.jnlp.

f. En la ventana de descarga de archivos, realice los siguientes pasos:

i. Instale la versión más reciente de JRE 1.6 en el cliente de Windows.

ii. Verifique que Java se haya instalado ejecutando el siguiente comando: java -version

La salida debe indicar Java versión 1.6.0_24 (Java 1.6) o posterior.

iii. Cambie la configuración de Windows para abrir siempre archivos con extensión jnlp con el programa Java Web Start Launcher.

Los pasos para cambiar la configuración de Windows varían en función de la versión de Windows que esté utilizando.

iv. Introduzca la URL de SnapManager que ha especificado en el paso 1.

La descarga de SnapManager se inicia en el cliente Windows y aparece un cuadro de diálogo Advertencia - Seguridad.

g. Siga estos pasos.

El contenido del mensaje y las etiquetas de los botones varían según la plataforma.

i. En el cuadro de diálogo Advertencia - Seguridad, haga clic en **Sí**.

Aparecerá un cuadro de diálogo.

ii. En el cuadro de diálogo falta de coincidencia del nombre de host, haga clic en **Ejecutar**.

Se muestra el cuadro de diálogo Advertencia - Seguridad con un mensaje acerca de la firma de la aplicación SnapManager.

iii. Haga clic en **Ejecutar**.

Un cuadro de diálogo con el título Java Installer - Advertencia de seguridad y el mensaje Warning Security - la firma digital de la aplicación tiene un error. ¿Desea ejecutar la aplicación?

iv. Haga clic en **Ejecutar**.

El explorador descarga e inicia la interfaz gráfica de usuario de SnapManager para Oracle.

Verificación del entorno

Puede verificar el entorno para asegurarse de que SnapDrive y SnapManager están configurados correctamente.

Descargue, instale y configure los requisitos previos necesarios. Asegúrese de que SnapManager esté instalado y que el servidor host esté ejecutándose.

1. Para verificar que SnapDrive está instalado y se puede ejecutar desde la cuenta raíz, ejecute el siguiente comando: Verificación del sistema smo

Información relacionada

El comando smo system verify

Verificando SnapDrive para Windows

Si ha instalado SnapDrive para Windows, compruebe que puede crear una copia Snapshot antes de utilizar SnapManager.

1. En el menú Inicio, haga clic con el botón derecho del ratón en **Mi PC** y seleccione **Administrar**.
2. En la ventana Administración de equipos, haga clic en **almacenamiento** > **SnapDrive**.
3. Seleccionar un disco.

   Consulte la *SnapDrive for Windows Guía de instalación y administración* para obtener más información acerca del uso de SnapDrive.

   Si ha encontrado correctamente información sobre el disco para el producto SnapDrive, SnapDrive funciona correctamente.

Información relacionada

"*SnapDrive for Windows Installation and Administration Guide*: mysupport.netapp.com/documentation/productsatoz/index.html"

Creación de repositorios

SnapManager requiere un repositorio en un host para conservar datos acerca de las operaciones que se realizan.

Asegúrese de que se han completado las siguientes tareas:

1. Cree un usuario y una contraseña de Oracle en la base de datos del repositorio.
2. Autorizar el acceso de los usuarios al repositorio.

Para un repositorio, SnapManager para Oracle requiere un tamaño de bloque mínimo de 4K para el espacio de tablas en el que está instalado. Puede comprobar el tamaño de bloque con el siguiente comando de SQL:

```
select a.username, a.default_tablespace, b.block_size
from dba_users a, dba_tablespaces b
a.username = repo_user
```

donde

- a.default_tablespace = b.tablespace_name
- a.username = el nombre de usuario en el repositorio

Si va a actualizar repositorios, debe reiniciar el servidor SnapManager para reiniciar todas las programaciones asociadas.

1. Para crear el repositorio, introduzca el comando create repository, utilizando el siguiente formato general: smo Repository create -repository -dbname repo_service_name -host repo_host -login -username repo_username -Port repo_Port-force] [-noprompt] [-quiet | -verbose]

Donde:

- -repository -dbname es el nombre de la base de datos del repositorio.
- -host es el nombre del host para el repositorio.
- -username es el nombre del usuario de la base de datos que tiene acceso al repositorio.
- -port es el puerto para el host. Las demás opciones para este comando son las siguientes:

  [-force] [-noprompt]

+ NOTA: Si tiene un repositorio existente con el mismo nombre y utiliza la opción -force , se sobrescribirán todos los datos de un esquema de repositorio existente.

Crear un repositorio

La siguiente línea de comandos crea un repositorio.

```
smo repository create -repository -dbname HRDP
-host server1 -login -username admin -port 1521
```

Cómo organizar repositorios

Puede organizar los repositorios de SnapManager para satisfacer las necesidades de su empresa. Puede organizarlos de varias maneras, incluso por tipo de aplicación y uso.

Puede organizar repositorios de varias maneras. Dos de estas maneras son:

Tipo	Características

Por aplicación	Si tiene varias bases de datos de Oracle que ejecutan diferentes aplicaciones, puede crear un repositorio de SnapManager para cada tipo de aplicación. Cada repositorio de SnapManager tendría perfiles para las bases de datos de un tipo de aplicación en particular. Todas las bases de datos de producción, desarrollo y pruebas de ese tipo de aplicación se gestionarían mediante el mismo repositorio de SnapManager. Esta opción ayudaría a agrupar bases de datos similares y a facilitar la clonación. Sin embargo, si tiene varios tipos de aplicaciones, es posible que tenga que gestionar varios repositorios de SnapManager y, si decide implementar otro tipo de aplicación, deberá crear otro repositorio de SnapManager. Como estos repositorios SnapManager gestionarán bases de datos de producción, cada uno de estos repositorios debe estar en un servidor con alta disponibilidad, lo cual puede resultar caro. Además, el tener que gestionar bases de datos de producción junto con bases de datos de desarrollo y prueba del mismo tipo en el mismo repositorio de SnapManager puede ser un problema de seguridad.
Por uso	Puede distribuir las bases de datos entre los repositorios de SnapManager en función de su uso (por ejemplo, producción, desarrollo, pruebas y formación). Esta opción limita el número de repositorios a los diferentes tipos de bases de datos que tiene. Dado que un único repositorio de SnapManager gestiona todas las bases de datos de producción, solo los administradores de las bases de datos de producción pueden acceder a este repositorio. Además, si decide implementar otra base de datos para un nuevo tipo de aplicación, sólo tendrá que registrar la base de datos en el repositorio de SnapManager correspondiente en lugar de crear un nuevo repositorio. La alta disponibilidad solo se puede proporcionar para el repositorio de SnapManager con los perfiles de todas las bases de datos de producción.

SnapManager para Oracle y SnapManager para SAP no deben compartir el mismo repositorio. Para SnapManager para Oracle y SnapManager para SAP, debe usar un repositorio diferente (un usuario de base de datos de Oracle diferente) para cada producto si las tiene en su entorno. El uso de un repositorio diferente, ya sea en la misma base de datos o en diferentes, ofrece más flexibilidad al permitir ciclos de actualización independientes para cada producto.

Orden de realización de operaciones

SnapManager le permite realizar diversas operaciones, como la creación de perfiles, la realización de backups y la clonado de backups. Estas operaciones deben realizarse en un orden específico.

1. Crear un perfil en un almacén existente mediante el comando smo profile create.

   > El usuario de Oracle especificado para la base de datos de destino debe tener privilegios de sysdba.

   En el siguiente ejemplo se muestra el comando para crear un perfil:

   ```
   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. Crear un backup en un perfil existente con el comando smo backup create.

   En el ejemplo siguiente se muestra el comando para crear un backup:

   ```
   smo backup create -profile prof1 -full -offline -label full_backup_prof1
   -force
   ```

3. Restaurar y recuperar un backup de base de datos en el almacenamiento primario mediante el comando smo backup restore.

   El ejemplo siguiente muestra el comando para restaurar un backup:

   ```
   smo backup restore -profile prof1 -label full_backup_prof1
   -complete -recover -alllogs
   ```

4. Crear una especificación de clon con el comando de plantilla de clon de smo.

   Puede utilizar el asistente Clone de la interfaz gráfica de usuario (GUI) para crear una especificación del clon de plantilla. También puede crear el archivo de especificación del clon mediante un editor de texto.

5. Clonar una base de datos con un backup existente mediante el comando smo clone create.

   Debe tener una especificación de clon existente o crear una especificación de clon para especificar las especificaciones de almacenamiento y base de datos del clon.

   En el ejemplo siguiente se muestra el comando para crear un clon:

   ```
   smo clone create -profile prof1 -backup-label full_backup_prof1
   -newsid clone1 -label prof1_clone -clonespec
   C:\\clone_spec\\prof1_clonespec.xml
   ```

Seguridad y gestión de credenciales

Puede gestionar la seguridad en SnapManager aplicando autenticación de usuario. El método de autenticación de usuario permite acceder a recursos como repositorios, hosts y perfiles.

Cuando se realiza una operación mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario (GUI), SnapManager recupera las credenciales establecidas para repositorios y perfiles. SnapManager guarda las credenciales de instalaciones anteriores.

El repositorio y los perfiles se pueden proteger con una contraseña. Una credencial es la contraseña configurada para el usuario de un objeto y la contraseña no está configurada en el objeto en sí.

Puede gestionar la autenticación y las credenciales realizando las siguientes tareas:

- Gestione la autenticación de usuarios mediante mensajes de contraseña en las operaciones o mediante el uso del comando smo credential set.

  Configurar credenciales para un repositorio, host o perfil.

- Vea las credenciales que rigen los recursos a los que tiene acceso.
- Borre las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Eliminar credenciales de un usuario para recursos individuales (hosts, repositorios y perfiles).

> Si la base de datos del repositorio está en un host de Windows, tanto el usuario local como el administrador y el usuario de dominio deben tener las mismas credenciales.

Qué es la autenticación de usuario

SnapManager autentica al usuario por medio de un inicio de sesión en el sistema operativo (SO) en el host en el que se ejecuta el servidor de SnapManager. Se puede habilitar la autenticación de usuario mediante mensajes de contraseña en las operaciones o mediante la credencial de smo se puede habilitar la autenticación de usuarios a través de mensajes de contraseña en las operaciones o mediante el comando smo credential set.

Los requisitos de autenticación de usuario dependen de dónde se realice la operación.

- Si el cliente SnapManager está en el mismo servidor que el host SnapManager, se autenticará mediante las credenciales del sistema operativo.

  No se le solicita una contraseña porque ya ha iniciado sesión en el host donde se ejecuta el servidor SnapManager.

- Si el cliente SnapManager y el servidor SnapManager están en hosts diferentes, SnapManager debe autenticarse con ambas credenciales de sistema operativo.

  SnapManager solicita contraseñas para cualquier operación si no se guardaron las credenciales del sistema operativo en la caché de credenciales del usuario SnapManager. Si introduce el comando smo credential set -host, guarde las credenciales del sistema operativo en el archivo de la caché de credenciales de SnapManager, de modo que SnapManager no solicita la contraseña de ninguna

operación.

Si está autenticado con el servidor SnapManager, se considera el usuario efectivo. El usuario efectivo para cualquier operación debe ser una cuenta de usuario válida en el host donde se ejecuta la operación. Por ejemplo, si ejecuta una operación de clonado, debe poder iniciar sesión en el host de destino del clon.

> SnapManager para Oracle podría fallar al autorizar a los usuarios creados en Servicios de Active Directory central, como LDAP y ANUNCIOS. Para asegurarse de que la autenticación no falla, debe establecer auth.disableServerAuthorization configurable en true.

Como usuario eficaz, puede gestionar las credenciales de las siguientes maneras:

- De manera opcional, es posible configurar SnapManager para almacenar credenciales de usuario en el archivo de credenciales de usuario de SnapManager.

  De manera predeterminada, SnapManager no almacena las credenciales del host. Puede resultar conveniente cambiar esto, por ejemplo, si tiene scripts personalizados que requieren acceso en un host remoto. La operación de clonado remoto es un ejemplo de una operación SnapManager que necesita las credenciales de inicio de sesión de un usuario para un host remoto. Para que SnapManager recuerde las credenciales de inicio de sesión de host del usuario en la caché de credenciales de usuario de SnapManager, establezca la propiedad host.credential.persists en TRUE en el archivo smo.config.

- Puede autorizar el acceso de los usuarios al repositorio.
- Puede autorizar el acceso de los usuarios a los perfiles.
- Es posible ver todas las credenciales de usuario.
- Es posible borrar las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Es posible eliminar credenciales de recursos individuales (hosts, repositorios y perfiles).

Almacenamiento de contraseñas cifradas para secuencias de comandos personalizadas

De forma predeterminada, SnapManager no almacena credenciales de host en la caché de credenciales de usuario. Sin embargo, puede cambiar esto. Puede editar el archivo smo.config para permitir el almacenamiento de las credenciales de host.

El archivo smo.config está ubicado en <default installation location>\properties\smo.config

1. Edite el archivo smo.config.
2. Configure host.credenciales.persista en TRUE.

Autorizando el acceso al repositorio

SnapManager permite configurar credenciales para que los usuarios de la base de datos accedan al repositorio. Con las credenciales, puede restringir o evitar el acceso a hosts, repositorios, perfiles y bases de datos de SnapManager.

Si ha configurado las credenciales con el comando set de credenciales, SnapManager no le solicita una contraseña.

Es posible configurar credenciales de usuario al instalar SnapManager o una versión posterior.

1. Introduzca el siguiente comando:

   conjunto de credenciales de smo -repository -dbname repo_service_name -host repo_host -login -username repo_username [-password repo_password] -port repo_port

Autorizando el acceso a los perfiles

SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

1. Introduzca el siguiente comando: smo credential set -profile -name profile_name [-password]

Información relacionada

El comando smo credential set

Visualización de las credenciales de usuario

Puede enumerar los hosts, perfiles y repositorios a los que tiene acceso.

1. Para enumerar los recursos a los que tiene acceso, escriba este comando: Lista de credenciales de smo

Ejemplo de visualización de credenciales de usuario

En este ejemplo, se muestran los recursos a los que tiene acceso.

```
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
```

Información relacionada

El comando smo credential list

Borrar credenciales de usuario para todos los hosts, repositorios y perfiles

Puede borrar la caché de sus credenciales para recursos (hosts, repositorios y perfiles). Esto elimina todas las credenciales de recursos del usuario que ejecuta el comando. Después de borrar la caché, debe volver a autenticar las credenciales para obtener acceso a estos recursos protegidos.

1. Para borrar sus credenciales, introduzca el comando smo credential clear en la CLI de SnapManager o seleccione **Admin** > **credenciales** > **Clear Cache** en la GUI de SnapManager.
2. Salga de la interfaz gráfica de usuario de SnapManager.

   NOTA:

   - Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager.
   - Si borró la caché de credenciales de la interfaz de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager.
   - Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar de nuevo la interfaz gráfica de usuario de SnapManager.
3. Para volver a configurar las credenciales, repita el proceso con el fin de establecer las credenciales para el repositorio, el host del perfil y el perfil. Para obtener información adicional sobre cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales tras borrar caché de credenciales".

Información relacionada

El comando smo credential clear

Configuración de credenciales después de borrar la caché de credenciales

Después de borrar la caché para quitar las credenciales de usuario almacenadas, puede configurar las credenciales para hosts, repositorios y perfiles.

Debe asegurarse de establecer las mismas credenciales de usuario para el repositorio, el host del perfil y el perfil que había especificado anteriormente. Se crea un archivo de credenciales cifrado al configurar las credenciales de usuario.

El archivo de credenciales se encuentra en C:\Documents and Settings\Administrator\Application Data\NetApp\smo\3.3.0.

Desde la interfaz gráfica de usuario (GUI) de SnapManager, si no hay ningún repositorio en repositorios, realice los siguientes pasos:

1. Haga clic en **tareas** > **Agregar repositorio existente** para agregar un repositorio existente.
2. Ejecute los siguientes pasos para configurar las credenciales del repositorio:
   a. Haga clic con el botón derecho del ratón en el repositorio y seleccione **Abrir**.
   b. En la ventana Repository Credentials Authentication, introduzca las credenciales de usuario.
3. Realice los siguientes pasos para configurar las credenciales del host:
   a. Haga clic con el botón derecho del ratón en el host bajo el repositorio y seleccione **Abrir**.
   b. En la ventana Host Credentials Authentication, introduzca las credenciales de usuario.

4. Realice los siguientes pasos para configurar las credenciales del perfil:
    a. Haga clic con el botón derecho del ratón en el perfil bajo el host y seleccione **Abrir**.
    b. En la ventana Profile Credentials Authentication, introduzca las credenciales de usuario.

Eliminación de credenciales para recursos individuales

Puede eliminar las credenciales de uno de los recursos protegidos, como un perfil, un repositorio o un host. De este modo, puede quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario de todos los recursos.

Información relacionada

El comando smo credential delete

Eliminación de credenciales de usuario para repositorios

Es posible eliminar las credenciales para que un usuario ya no pueda acceder a un repositorio en particular. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario para todos los recursos.

1. Para eliminar las credenciales de repositorio de un usuario, introduzca este comando:credencial de smo delete -repository-dbnamerepo_service_name-hostrepo_host-login -usernamerepo_username -portrepo_Port

Eliminación de credenciales de usuario para hosts

Es posible eliminar las credenciales de un host para que un usuario ya no pueda acceder a él. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar todas las credenciales del usuario para todos los recursos.

1. Para eliminar las credenciales de host de un usuario, introduzca este comando:credencial de smo delete -host-namehost_name-username-username

Eliminación de credenciales de usuario para perfiles

Es posible eliminar las credenciales de usuario de un perfil para que un usuario ya no pueda acceder a él.

1. Para eliminar las credenciales de perfil de un usuario, introduzca este comando: smo credential delete -profile-nameprofile_name

Gestionar perfiles para backups eficientes

Debe crear un perfil en SnapManager para la base de datos donde desea realizar una operación. Debe seleccionar el perfil y, a continuación, seleccionar la operación que desea realizar.

Tareas relacionadas con perfiles

Es posible realizar las siguientes tareas:

- Cree perfiles para habilitar backups y backups completos o parciales en almacenamiento primario o secundario.

  También es posible crear perfiles para separar los backups de registros de archivo de los backups de archivos de datos.

- Verificar perfiles.
- Actualizar perfiles.
- Eliminar perfiles.

Acerca de los perfiles y la autenticación

Al crear un perfil, puede especificar una base de datos y elegir uno de los siguientes métodos para conectarse a la base de datos:

- Autenticación de Oracle con un nombre de usuario, contraseña y puerto
- Autenticación del sistema operativo (SO) sin nombre de usuario, contraseña ni puerto.

  Para la autenticación del sistema operativo, debe introducir la información de usuario y del grupo de cuenta del sistema operativo.

- Autenticación de base de datos cuando sqlnet.authentication_services está establecido en NONE. A continuación, SnapManager utiliza el nombre de usuario y la contraseña de la base de datos para todas las conexiones con la base de datos de destino. SnapManager también puede utilizar la autenticación nativa de Windows cuando sqlnet.authentication_services se establece en NTS.

Puede establecer sqlnet.authentication_services a NINGUNO solo en los siguientes entornos:

Distribución de la base de datos	Versión de Oracle	Es compatible con la autenticación de la base de datos de destino
Cualquier base de datos que no sea ASM y que no sea RAC	Oracle 10g y Oracle 11g (inferior a 11.2.0.3)	Sí

Nota: después de deshabilitar sqlnet.authentication_services y cambiar el método de autenticación a autenticación de base de datos, debe establecer sqlnet.authentication_services en NINGUNO.

Si accede a un perfil por primera vez, debe introducir la contraseña de su perfil. Después de introducir sus credenciales, es posible ver los backups de la base de datos dentro del perfil.

Información relacionada

Qué perfiles son

Creación de perfiles

Al crear perfiles, puede asignar una cuenta de usuario de base de datos Oracle concreta al perfil. Puede establecer la política de retención para el perfil y establecer el recuento

de retención y la duración de cada clase de retención.

Si no se proporcionan los valores de los parámetros -login, -password y -Port de la base de datos, el modo de autenticación del sistema operativo utiliza las credenciales predeterminadas.

Al crear un perfil, SnapManager realiza una comprobación de elegibilidad de restauración para determinar el mecanismo de restauración que puede usarse para restaurar la base de datos.

SnapManager (3.2 o posterior) permite separar los archivos de registro de archivos de los archivos de datos al crear un nuevo perfil o actualizar un perfil existente. Después de separar el backup con el perfil, se puede crear únicamente el backup de los archivos de datos o el backup de solo registro del archivo de la base de datos. Se puede usar el nuevo perfil o el perfil actualizado para crear el backup que contiene tanto los archivos de datos como los archivos de registro de archivos. Sin embargo, no se puede utilizar el perfil para crear el backup completo ni revertir la configuración.

Perfiles para crear copias de seguridad completas y parciales

Es posible crear perfiles para crear un backup completo de la base de datos que contenga los archivos de datos, los archivos de control, los archivos de registro de archivos y el backup parcial de la base de datos que contenga los archivos de datos o espacios de tablas especificados, todos los archivos de control y todos los archivos de registro de archivos. SnapManager no permite crear backups de registros de archivos independientes con los perfiles creados para backups completos y parciales.

Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad sólo archivogs

Al crear un nuevo perfil, puede incluir -separate-archivvelog-backups para separar el backup del registro de archivo del backup del archivo de datos. También puede actualizar el perfil existente para separar la copia de seguridad del archivo de datos.

Al usar las opciones nuevas de perfil para separar los backups de los registros de archivos, es posible realizar las siguientes operaciones de SnapManager:

- Cree un backup de registro de archivos
- Eliminar un backup de registro de archivos
- Montar un backup de registro de archivos
- Liberar un backup de registro de archivo

Al crear el perfil para separar los backups de registros de archivos del backup de archivos de datos, si los archivos de registro de archivos no existen en la base de datos para la que se creó el perfil, no existe un archivo de registro archivado con mensaje de advertencia en el sistema de archivos activo. Las versiones del archivo de registro archivado anteriores al archivo de registro de <archive log thread version> no se incluirán en el backup. Incluso si se crean backups para esta base de datos, los archivos de registro de archivos no están disponibles en los backups de la base de datos.

> Si se produce un error al crear un perfil, utilice el comando smosystem dump. Después de crear un perfil, si se encuentra con un error, utilice los comandos dump y smofrofile dump de operación.

1. Para crear un perfil con un nombre de usuario, una contraseña y un puerto (autenticación de Oracle), introduzca el comando siguiente: smo-profile create -profileprofile [-profile-passwordprofile_password] -repository-dbnamerepo_dbname-condrostrepo_host-portrepo_port-login-usernamerepo] [-nombre-nombre-nombre-usuario_correo_e] [-nombredeusuario_correo-did] [-nombre_correo-di_archivo]-did]-

diserondnnombre_correo-correo-archivo] [-di_correo-di_correo-di_correo-di_archivo]]-diserondrb]

Las demás opciones para este comando son las siguientes:

[-force] [-noprompt]

También puede incluir otras opciones al crear perfiles, dependiendo de cómo desee tener acceso a la base de datos.

Si…	Realice lo siguiente…
Desea utilizar la autenticación de base de datos para crear un perfil	Especifique los detalles de inicio de sesión de la base de datos.
Desea especificar una política de retención de copias de seguridad para copias de seguridad	Especifique el recuento de retención o la duración de una clase de retención, o ambos. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). • -hourly es la clase de retención por hora, para la cual [-count n] [-duration m] son el recuento de retención y la duración de la retención, respectivamente. • -daily es la clase de retención diaria, para la cual [-count n] [-durationm] son el recuento de retención y la duración de la retención, respectivamente. • -weekly es la clase de retención semanal, para la cual [-count n] [-duration m] son el recuento de retención y la duración de la retención, respectivamente. • -monthly es la clase de retención mensual, para la cual [-count n] [-durationm] son el recuento de retención y la duración de la retención, respectivamente.

Desea activar la notificación por correo electrónico para el estado de finalización de las operaciones de la base de datos	Especifique las siguientes opciones y variables: • -summary-notification permite configurar una notificación de correo electrónico de resumen para varios perfiles en una base de datos de repositorio. • -notification permite recibir una notificación por correo electrónico del estado de finalización de la operación de base de datos de un perfil. • -success-emailemail_address2 le permite recibir una notificación por correo electrónico sobre la operación correcta de la base de datos mediante un perfil nuevo o existente. • -failure-emailemail_address2 le permite recibir una notificación por correo electrónico sobre la operación de la base de datos fallida realizada mediante un perfil nuevo o existente. • -subjectsubject_text especifica el texto del asunto para la notificación de correo electrónico al crear un perfil nuevo o uno existente. Si los ajustes de notificación no están configurados para el repositorio y se intentan configurar las notificaciones de perfil o resumen mediante la CLI, se registra el siguiente mensaje en el registro de consola: SMO-14577: Notification Settings no configurado. Si ha configurado la configuración de notificación e intenta configurar la notificación de resumen utilizando la CLI sin habilitar la notificación de resumen para el repositorio, se muestra el siguiente mensaje en el registro de consola: SMO-14575: La configuración de notificación de resumen no está disponible para este repositorio_**_

Desea hacer una copia de seguridad de los archivos de registro de archivos por separado de los archivos de datos	Especifique las siguientes opciones y variables: • -separar-archivvelog-backups permite separar el backup de registros de archivo del backup del archivo de datos. • -retain-archivvelog-backups establece la duración de la retención para los backups de registros de archivos. Debe especificar una duración de retención positiva. Los backups de los registros de archivos se conservan según la duración de retención de los registros de archivo. Los backups de los archivos de datos se retienen en función de las políticas de retención existentes. • -include-with-online-backups incluye el backup de registros de archivos junto con el backup de base de datos en línea. Esta opción permite crear un backup de archivos de datos en línea y un backup de registros de archivos juntos para el clonado. Cuando se configura esta opción, siempre que se crea un backup de archivos de datos en línea, se crean los backups de los registros de archivos junto con los archivos de datos inmediatamente. • -no-include-with-online-backups no incluye el backup de registros de archivo junto con el backup de base de datos.
Puede recopilar los archivos de volcado después de que la operación de creación de perfil se haya realizado correctamente	Especifique la opción -dump al final del comando profile create.

Información relacionada

Cómo recopilar archivos de volcado

Nomenclatura de copias Snapshot

Puede especificar una convención o un patrón de nomenclatura para describir las copias de Snapshot relacionadas con el perfil que crea o actualiza. También puede incluir texto personalizado en todos los nombres de copias de Snapshot.

Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias Snapshot que todavía no se han producido; las copias Snapshot que existen conservan el patrón de snapname anterior.

Los siguientes ejemplos muestran los dos nombres de copias Snapshot tomados de un volumen. La segunda copia snapshot que se muestra tiene *F_H_1* en la mitad de su nombre. El "1" indica que es la primera copia snapshot tomada en el conjunto de backup. La primera copia Snapshot enumerada es la más reciente y tiene una «2», lo que significa que se toma la segunda copia Snapshot. La copia Snapshot "1" incluye los archivos de datos; la copia Snapshot "2" incluye los archivos de control. Dado que las copias snapshot del archivo de control deben realizarse después de realizar la copia snapshot del archivo de datos, se necesitan dos copias snapshot.

```
smo_profile_sid_f_h_2_8ae482831ad14311011ad14328b80001_0
smo_profile_sid_f_h_1_8ae482831ad14311011ad14328b80001_0
```

El patrón predeterminado incluye el smid requerido, como se muestra en la siguiente:

- Patrón predeterminado: smo_{profile}_{dB-sid}_{scope}_{mode}_{smid}
- Ejemplo: smo_my_profile_rac51_f_h_2_8abc01e915a55ac50115a55acc8d0001_0

Es posible usar las siguientes variables en el nombre de la copia Snapshot:

Nombre de la variable	Descripción	Valor de ejemplo
smid (obligatorio)	El ID único de SnapManager es el único elemento requerido cuando se crea un nombre para la copia Snapshot. Este ID garantiza la creación de un nombre de snapshot único.	8abc01e915a55ac50115a55ac8d0001_0
Clase (opcional)	Clase de retención asociada al backup para el perfil e indicada por cada hora (h), día (d), semanal (w), mensual (m) o ilimitado (u).	d
Comentario (opcional)	Comentario asociado al backup del perfil. Los espacios en este campo se convertirán en guiones bajos cuando se complete el nombre de la copia Snapshot.	sample_comment_spaces_reemplazado
Fecha (opcional)	Fecha en la que se realiza la copia de seguridad para el perfil. Los valores de fecha se rellenarán con ceros si es necesario. (aaaammdd)	20070218
db-host (opcional)	Nombre de host de la base de datos asociado con el perfil que se va a crear o actualizar.	mi_host

db-name (opcional)	Nombre de la base de datos asociada con la copia de Snapshot que crea.	rac5
db-sid (opcional)	sid de base de datos asociado con la copia de Snapshot que crea.	racer51
Etiqueta (opcional)	Etiqueta asociada al backup para el perfil.	etiqueta_muestra
Modo (opcional)	Especifica si el backup se completa en línea (h) o sin conexión (c).	h
Perfil (opcional)	El nombre del perfil asociado con el backup que cree.	mi_perfil
Alcance (opcional)	Especifica si el backup está completo (f) o parcial (p).	f
Tiempo (opcional)	Hora a la que se produce el backup para el perfil. Los valores de hora de esta variable utilizan el reloj de 24 horas y están acolchados con ceros si es necesario. Por ejemplo, 5:32 y 8 segundos se muestran como 053208 (hhmmss).	170530
Zona horaria (opcional)	Zona horaria especificada para el host de la base de datos de destino.	EST
Usertext (opcional)	Texto personalizado que puede introducir.	prod

Nota: SnapManager para Oracle no admite el símbolo de dos puntos (:) en las formas largas de los nombres de las copias Snapshot.

Cambiar el nombre de los perfiles

SnapManager le permite cambiar el nombre del perfil al actualizar el perfil. Las funcionalidades de SnapManager establecidas en el perfil y las operaciones que se pueden realizar antes de cambiar de nombre se conservan para el perfil cuyo nombre ha cambiado.

- Debe asegurarse de que no haya operaciones SnapManager en ejecución en el perfil mientras cambia el nombre del perfil.

Es posible cambiar el nombre del perfil tanto en la interfaz de línea de comandos (CLI) de SnapManager como en la interfaz gráfica de usuario (GUI). Al actualizar el perfil, SnapManager verifica y actualiza el nombre del

perfil en el repositorio.

> SnapManager no admite cambiar el nombre del perfil en la ventana de actualización de varios perfiles.

Cuando proporcione un nuevo nombre de perfil, el nuevo nombre de perfil se añadirá a la caché de credenciales del cliente y se eliminará el nombre del perfil anterior. Al cambiar el nombre del perfil desde un cliente, sólo se actualiza la caché de credenciales de ese cliente. Debe ejecutar el comando smo profile SYNC desde cada cliente para actualizar la nueva caché de credenciales con el nombre del nuevo perfil.

Puede establecer la contraseña del perfil mediante el comando smo credential set.

Si se incluyó el nombre de perfil en un patrón de nomenclatura de copias Snapshot, al cambiar el nombre de un perfil, se actualiza el nuevo nombre del perfil. Todas las operaciones SnapManager que se realizan en el perfil utilizan el nuevo nombre del perfil. Los backups creados con el perfil anterior siguen teniendo el nombre del perfil anterior y se usan para realizar otras operaciones de SnapManager.

Si va a realizar la actualización gradual de los hosts del servidor SnapManager, debe asegurarse de realizar la actualización completa antes de cambiar el nombre del perfil.

El nuevo nombre del perfil sólo se actualiza desde el cliente SnapManager desde el que se realiza la solicitud. Los clientes SnapManager conectados al servidor SnapManager no reciben notificaciones sobre el cambio en el nombre del perfil. Puede comprobar el registro de operaciones para conocer el cambio en el nombre del perfil.

> Si una operación de backup programada comienza en el momento de cambiar el perfil, entonces se produce un error en la operación programada.

1. Introduzca el siguiente comando: smo profile update -profileprofile [-new-profilenew_profile_name]

Cambio de contraseñas de perfil

Para proteger los perfiles existentes en el repositorio, debe actualizar las contraseñas de los perfiles. Puede aplicar esta contraseña actualizada al crear una copia de seguridad con este perfil.

1. Para actualizar la contraseña de perfil de un perfil existente, escriba este comando:

   actualización del perfil de smo -profile_name -profile-password

Información relacionada

El comando smo profile update

Restablecimiento de la contraseña del perfil

Puede restablecer la contraseña del perfil si no recuerda la contraseña que ha proporcionado al crear el perfil.

- Debe asegurarse de que el servidor SnapManager esté en ejecución en la base de datos del repositorio.
- Debe tener las credenciales de administrador local del host en el que reside la base de datos del repositorio.

- Debe asegurarse de que el perfil no esté en uso para ninguna operación cuando se restablezca la contraseña para ese perfil.

Puede restablecer la contraseña desde la interfaz de línea de comandos o desde la interfaz gráfica de usuario de SnapManager. Al restablecer la contraseña, SnapManager consulta al servidor SnapManager en el host de repositorios para identificar el sistema operativo para el host de repositorios. Debe introducir las credenciales de usuario autorizado para conectarse con el host de repositorios. El servidor SnapManager autentica a los usuarios con sus credenciales de administrador local en la base de datos de repositorios. Cuando la autenticación se realiza correctamente, SnapManager restablece la contraseña del perfil en el servidor SnapManager con la nueva contraseña.

SnapManager no mantiene el historial de las operaciones de restablecimiento de contraseña.

1. Restablezca la contraseña de perfil. Para ello, introduzca el siguiente comando: smo password reset -profeprofile [-profile-passwordprofile_password] [-Repository-hostadmin-passwordadmin_password]

Autorizando el acceso a los perfiles

SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

1. Introduzca el siguiente comando: smo credential set -profile -name profile_name [-password]

Información relacionada

El comando smo credential set

Verificando perfiles

Puede comprobar que un perfil existente está configurado correctamente. Cuando se verifica un perfil, SnapManager comprueba si el entorno del perfil que se ha especificado y verifica que el perfil está configurado y que la base de datos de este perfil esté accesible.

1. Para comprobar si el perfil está configurado correctamente, introduzca este comando: smo profile verify -profile_name

Información relacionada

El comando smo profile verify

Actualizando perfiles

Puede actualizar los perfiles para modificar la contraseña del perfil, la cantidad de backups que se deben retener, el acceso a la base de datos, la autenticación del sistema operativo (SO) con la autenticación de la base de datos y viceversa, e información sobre el host. Si cambia la información de contraseña de la base de datos Oracle, también debe cambiar esa información en el perfil.

SnapManager (3.2 o posterior) permite actualizar el perfil para separar los backups de registros de archivos de los backups de archivos de datos con la opción -separate-archivvelog-backups. Es posible especificar una

duración de retención separada para el backup del registro de archivo. SnapManager le permite incluir el backup de registros de archivos junto con el backup de base de datos en línea. También puede crear un backup de archivo de datos en línea y un backup de registro de archivo juntos para clonar. Cuando se crea un backup de archivos de datos en línea, los backups de registros de archivos se crean inmediatamente junto con los archivos de datos.

1. Introduzca el siguiente comando: archivo-nod-pattern -profileprofile [-new-profilenew_profile_name] [-profile-passwordprofile_password][-database-dbnamedb_dbname-host_host] [-siddb_sid] [-login -nombrenamedb_nombre_usuario_contraseña] [_usuario_archivo]]-nombre_archivo] [-archivo-archivo-archivo-archivo]]-archivo-archivo-archivo-archivo] [-archivo-archivo-archivo-archivo-archivo-archivo]-archivo-archivo-archivo] [-archivo-archivo-archivo-archivo-archivo-archivo-archivo-archivo]]-archivo-archivo-archivo-archivo] [_archivo-archivo-archivo-archivo-archivo-archivo-archivo]-archivo-archivo-archivo-archivo-archivo-archivo]] [_archivo-archivo-archivo-archivo-archivo] [_archivo-archivo]-archivo-archivo-archivo-archivo-archivo-archivo-archivo]-archivo]-archivo] [_archivo-archivo]-archivo-archivo-archivo] [_archivo-archivo-archivo-archivo-archivo-archivo]-archivo] [

   Las demás opciones para este comando son las siguientes:

   [-force] [-noprompt]

Si desea…	Realice lo siguiente…
Cambiar la política de retención de copias de seguridad para copias de seguridad de la base de datos en el perfil	Especifique el recuento de retención o la duración de la retención para una clase de retención, o ambos, para cambiar la política de retención. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). • -hourly es la clase de retención por hora, para la que [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente. • -daily es la clase de retención diaria, para la cual [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente. • -weekly es la clase de retención semanal, para la cual [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente. • -mensual es la clase de retención mensual, para la que [-compensn] [-durationm]] son el recuento de retención y la duración de la retención, respectivamente.

Activar notificaciones por correo electrónico para el estado de finalización de las operaciones de la base de datos	Especifique las siguientes opciones y variables: • -summary-notification permite configurar una notificación de correo electrónico de resumen para varios perfiles en una base de datos de repositorio. • -notification permite recibir una notificación por correo electrónico sobre el estado de finalización de la operación de base de datos de un perfil. • -success-emailemail_dirección2 le permite recibir una notificación por correo electrónico tras la finalización de una operación de base de datos exitosa usando un perfil nuevo o existente. • -failure-emailemail_address2 le permite recibir una notificación por correo electrónico en una operación de base de datos fallida realizada mediante un perfil nuevo o existente. • -subjectsubject_text especifica el texto del asunto para la notificación de correo electrónico mientras se crea un perfil nuevo o un perfil existente. Si los ajustes de notificación no están configurados para el repositorio y intenta configurar las notificaciones de perfil o resumen mediante la interfaz de línea de comandos (CLI), se registra el siguiente mensaje en el registro de consola: SMO-14577: Notification Settings not configured. Si ha configurado la configuración de notificación y está intentando configurar la notificación de resumen utilizando la CLI sin habilitar la notificación de resumen para el repositorio, se registra el siguiente mensaje en el registro de consola: SMO-14575: Configuración de notificación de resumen no disponible para este repositorio_**

Actualice el perfil para crear una copia de seguridad de los archivos de registro de archivos por separado	Especifique las siguientes opciones y variables: • -separate-archivvelog-backups permite crear una copia de seguridad de los archivos de registro de archivos por separado de los archivos de la base de datos. Después de especificar esta opción, puede crear una copia de seguridad sólo de archivos de datos o una copia de seguridad sólo de archivvelogs. No es posible crear un backup completo. Además, no puede revertir la configuración del perfil separando la copia de seguridad. SnapManager conserva los backups según la política de retención de los backups que se crearon antes de usar un backup de solo archivado. • -retain-archivvelog-backups establece la duración de la retención para los backups de registros de archivos. Si actualiza el perfil por primera vez, puede separar los backups de registros de archivos del backup de archivos de datos con la opción -separate-archivvelog -backups; debe proporcionar la duración de retención para los backups de registros de archivos mediante la opción -retain -archivvelog-backups. La configuración de la duración de la retención es opcional cuando se actualiza el perfil más adelante. • -include-with-online-backups especifica que el backup de registros de archivos se incluye junto con el backup de base de datos. • -no-include-with-online-backups especifica el backup del archivo de registro de archivos no se incluye junto con el backup de base de datos.
Cambiar el nombre de host de la base de datos de destino	Especifique -hostnew_dB_host para cambiar el nombre de host del perfil.
Recopilar los archivos de volcado después de la operación de actualización de perfil	Especifique la opción -dump.

2. Para ver el perfil actualizado, escriba el siguiente comando: smo profile show

Información relacionada

Cómo recopilar archivos de volcado

Eliminar perfiles

Puede eliminar un perfil en cualquier momento, siempre que no contenga copias de seguridad correctas o incompletas. Es posible eliminar perfiles que contengan copias de seguridad liberadas o eliminadas.

1. Para eliminar un perfil, escriba este comando: smo profile delete -profile_name

Información relacionada

El comando smo profile delete

Realizar backups de bases de datos

SnapManager permite realizar backups de datos en recursos de almacenamiento local mediante secuencias de comandos de posprocesamiento.

SnapManager ofrece las siguientes opciones para realizar backups, restaurar y recuperar los datos de la base de datos:

- Realice una copia de seguridad de toda la base de datos o de una parte de ella.

  Si realiza una copia de seguridad de una parte de la misma, especifique un grupo de tablespaces o un grupo de archivos de datos.

- Realice una copia de seguridad de los archivos de datos y de los archivos de registro de archivo por separado.
- Realizar un backup de las bases de datos en el almacenamiento primario (también llamado almacenamiento local) y protegerlas mediante la realización de backups a sistemas secundarios mediante secuencias de comandos de posprocesamiento.
- Programar copias de seguridad rutinarias.

La diferencia entre SnapManager (3.2 o posterior) y las versiones anteriores de SnapManager

SnapManager (3.1 o anterior) permite crear backups completos de la base de datos que contienen archivos de datos, archivos de control y archivos de registro de archivos.

SnapManager (3.1 o anterior) solo administra los archivos de datos. Los archivos de registro de archivos se mantienen usando soluciones fuera de SnapManager.

SnapManager (3.1 o anterior) impone las siguientes restricciones en la gestión de los backups de las bases de datos:

- Impacto en el rendimiento

  Cuando se realiza un backup de base de datos en línea completo (cuando la base de datos está en modo

de backup), el rendimiento de la base de datos se reduce durante el periodo de tiempo hasta que se crea el backup. En SnapManager (3.2 o posterior), pueden realizarse backups de bases de datos limitados y backups frecuentes de registros de archivo. La realización de backups frecuentes de registros de archivos ayuda a evitar que la base de datos se coloque en modo de backup.

- Restauración y recuperación manuales

  Cuando los archivos de registro de archivos necesarios no existen en el sistema de archivos activo, los administradores de la base de datos deben identificar qué backup contiene los archivos de registro de archivos, montar los backups de la base de datos y recuperar la base de datos restaurada. Este proceso requiere mucho tiempo.

- Restricciones de espacio

  Cuando se crea un backup de la base de datos, los destinos de registro de archivos se llena, lo que hace que la base de datos no responda hasta que se crea espacio suficiente en el almacenamiento. En SnapManager (3.2 o posterior), se pueden quitar los archivos de registro de archivos del sistema de archivos activo para liberar espacio periódicamente.

Por qué son importantes las copias de seguridad de archivos de registro

Los archivos de registro de archivos son necesarios para avanzar la base de datos después de ejecutar una operación de restauración. Cada transacción en una base de datos Oracle se captura en los archivos archive log (si la base de datos está en el modo archive log). Los administradores de bases de datos pueden restaurar los backups de la base de datos con los archivos de registro de archivos.

Ventajas de las copias de seguridad archivvelog-only

- Proporciona una duración de retención independiente para backups de solo archivado

  Puede tener menos duración de retención para los backups de solo archivado que se requieren para la recuperación.

- Protege los backups de solo archivado mediante secuencias de comandos de posprocesamiento
- Mejora el rendimiento de la base de datos
- Consolida los backups de registros de archivos

  SnapManager consolida los backups de registros de archivos cada vez que se realiza un backup liberando las copias de seguridad duplicadas de los registros de archivo.

Qué son los backups de la base de datos SnapManager

SnapManager permite realizar distintas tareas de backup. Puede asignar clases de retención para especificar cuánto tiempo se puede retener la copia de seguridad; una vez alcanzado ese límite de tiempo, se elimina la copia de seguridad.

- Crear backups en el almacenamiento principal
- Cree backups protegidos en los recursos de almacenamiento secundario mediante scripts de postprocesamiento
- Compruebe que los backups se han realizado correctamente
- Ver una lista de backups

- Programar las copias de seguridad utilizando la interfaz gráfica de usuario
- Gestión de la cantidad de backups incorporados
- Libere recursos de backup
- Montar y desmontar backups
- Eliminar backups

SnapManager crea backups mediante una de las siguientes clases de retención:

- Cada hora
- Todos los días
- Semanal
- Mensual
- Ilimitada

Si se agregan nuevos archivos de datos a la base de datos, debe crear una copia de seguridad inmediatamente. Además, si restaura una copia de seguridad realizada antes de agregar los nuevos archivos de datos e intenta recuperarse a un punto después de agregar los nuevos archivos de datos, el proceso de recuperación automática podría fallar. Consulte la documentación de Oracle para obtener más información sobre el proceso de recuperación de los archivos de datos agregados después de una copia de seguridad.

Qué son los backups completos y parciales

Puede elegir hacer una copia de seguridad de toda la base de datos o sólo una parte de ella. Si decide realizar una copia de seguridad de una parte de la base de datos, puede optar por realizar una copia de seguridad de un grupo de tablespaces o archivos de datos. Puede optar por realizar un backup separado de los espacios de tablas y los archivos de datos.

En la siguiente tabla, se enumeran los beneficios y las consecuencias de cada tipo de backup:

Tipo de backup	Ventajas	Desventajas
Lleno	Minimiza el número de copias de Snapshot. Para los backups en línea, cada espacio de tabla está en modo de backup durante todo el tiempo que lleva la operación de backup. SnapManager toma una copia snapshot por cada volumen que utiliza la base de datos, además de una copia snapshot por cada volumen que ocupan los archivos de registro.	Para los backups en línea, cada espacio de tabla está en modo de backup durante todo el tiempo que lleva la operación de backup.

Parcial	Minimiza la cantidad de tiempo que cada espacio de tabla pasa en modo de backup. SnapManager agrupa las copias snapshot que toma por espacio de tabla. Cada espacio de tabla está en modo de backup solo suficientemente tiempo para crear las copias Snapshot. Este método de agrupación de las copias Snapshot minimiza las escrituras de bloque físico en los archivos de registro durante un backup en línea.	El backup puede requerir la creación de copias Snapshot de varios espacios de tablas en el mismo volumen. Este método puede provocar que SnapManager cree varias copias Snapshot de un solo volumen durante la operación de backup.

Nota: aunque puede realizar una copia de seguridad parcial, siempre debe realizar una copia de seguridad completa de toda la base de datos.

Los tipos de backup y la cantidad de copias de Snapshot

El tipo de backup (completo o parcial) afecta al número de copias Snapshot que crea SnapManager. Para un backup completo, SnapManager crea una copia snapshot de cada volumen, mientras que, para un backup parcial, SnapManager crea una copia snapshot de cada archivo de espacio de tabla.

> Data ONTAP limita el número máximo de copias snapshot a 255 por volumen. Solo puede alcanzar este máximo si configura SnapManager para retener un gran número de backups en los que cada backup esté compuesto por numerosas copias de Snapshot.

Para mantener un pool adecuado de backups disponible a la vez que garantiza que no se alcance el límite máximo de copias Snapshot por volumen, debe eliminar backups cuando ya no sean necesarios. Puede configurar la política de retención de SnapManager para eliminar los backups correctos después de alcanzar un umbral específico para una frecuencia de backup específica. Por ejemplo, una vez que SnapManager crea cuatro backups diarios correctos, SnapManager elimina los backups diarios creados en el día anterior.

En las siguientes tablas, se muestra cómo SnapManager crea copias Snapshot según el tipo de backup. El ejemplo de las tablas supone que la base de datos Z incluye dos volúmenes, cada volumen incluye dos tablespaces (TS1 y TS2) y cada tablespace incluye dos archivos de base de datos (ts1_1.dbf, ts1_2.dbf, ts2_1.dbf y ts2_2.dbf).

En estas tablas, se muestra cómo los dos tipos de backups producen diferentes cantidades de copias Snapshot.

SnapManager crea copias Snapshot a nivel de volumen en lugar del espacio de tabla, lo que reduce normalmente el número de copias Snapshot que debe crear.

> Ambos backups también crean copias Snapshot de los archivos de registro.

Volúmenes en la base de datos	Tablespace TS1 (incluye 2 archivos de base de datos)	Tablespace TS2 (incluye 2 archivos de base de datos)	Se crearon copias Snapshot	Número total de copias Snapshot

E:\datos	TS1_1.dbf	TS2_1.dbf	1 por volumen	2

Volúmenes en la base de datos	Tablespace TS1 (incluye 2 archivos de base de datos)	Tablespace TS2 (incluye 2 archivos de base de datos)	Se crearon copias Snapshot	Número total de copias Snapshot
E:\datos	TS1_1.dbf	TS2_1.dbf	2 por archivo	4

Backups completos en línea

Durante un backup online completo, SnapManager realiza un backup de toda la base de datos y crea copias Snapshot en el nivel del volumen (no en el nivel de espacio de tabla).

SnapManager crea dos copias Snapshot para cada backup. Si todos los archivos necesarios para la base de datos se encuentran en un único volumen, las dos copias de Snapshot aparecen en ese volumen.

Cuando se especifica un backup completo, SnapManager realiza las siguientes acciones:

1. Coloca toda la base de datos en el modo de copia de seguridad en línea
2. Crea copias snapshot de todos los volúmenes que contienen archivos de base de datos
3. Saca la base de datos del modo de backup en línea
4. Fuerza un conmutador de registro y, a continuación, archiva los archivos de registro

   Esto también vacía la información de redo en el disco.

5. Genera archivos de control de copia de seguridad
6. Crea una copia snapshot de los archivos de registro y los archivos de control de copia de seguridad

Cuando se realiza un backup completo, SnapManager coloca toda la base de datos en el modo de backup en línea. Un tablespace individual (por ejemplo, E:\data\ts1_1.dbf) está en el modo de copia de seguridad en línea más largo que ciertos tablespaces o archivos de datos que se han especificado.

Cuando una base de datos entra en modo de backup, Oracle escribe bloques completos en los registros y no se limita a escribir el delta entre backups. Como las bases de datos trabajan más en modo de backup en línea, elegir un backup completo supone una mayor carga en el host.

Aunque realizar backups completos supone una mayor carga en el host, los backups completos requieren menos copias Snapshot, lo que produce menos requisitos de almacenamiento.

Backups parciales en línea

En lugar de un backup completo, se puede optar por realizar un backup parcial de los espacios de tablas en una base de datos. Mientras SnapManager realiza una copia Snapshot de volúmenes para realizar backups *Full*, SnapManager realiza una copia Snapshot de cada espacio de tabla especificado para *parciales* backups.

Debido a que el nivel de tablespace es el nivel más bajo que Oracle permite en el modo de copia de seguridad, SnapManager procesa las copias de seguridad a nivel de tablespace, incluso si se especifica un archivo de datos en un tablespace.

Con un backup parcial, cada espacio de tabla existe en modo de backup durante un menor tiempo que en un backup completo. Durante un backup en línea, la base de datos siempre está disponible para los usuarios. No obstante, la base de datos debe realizar más trabajo y el host debe ejecutar más operaciones de I/o físicas Asimismo, debido a que se realizan copias Snapshot de cada espacio de tabla especificado o cada espacio de tabla que contiene un archivo de datos especificado en lugar de todo el volumen, SnapManager realiza más copias Snapshot.

SnapManager realiza copias Snapshot de espacios de tablas o archivos de datos específicos. El algoritmo de copia de seguridad parcial es un bucle que SnapManager repite hasta que ha tomado una copia snapshot de cada tablespace o archivo de datos especificado.

> Aunque se puede realizar un backup parcial, se recomienda realizar siempre un backup completo de toda la base de datos.

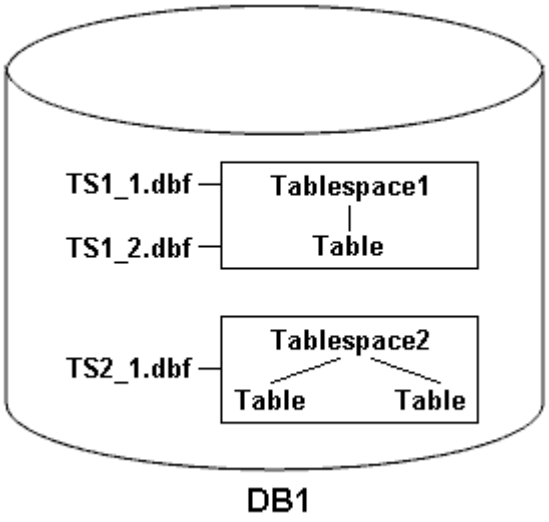
Durante un backup parcial, SnapManager realiza las siguientes acciones:

1. Coloca el tablespace que contiene los archivos de datos en modo de copia de seguridad.
2. Toma una copia Snapshot de todos los volúmenes utilizados por el espacio de tablas.
3. Quita el tablespace del modo de copia de seguridad.
4. Continúa este proceso, hasta que ha tomado una copia snapshot de todos los espacios de tablas o archivos.
5. Fuerza un conmutador de registro y, a continuación, archiva los archivos de registro.
6. Genera archivos de control de copia de seguridad.
7. Toma una copia snapshot de los archivos de registro y los archivos de control de copia de seguridad.

Ejemplos de operaciones de backup, restauración y recuperación

Puede encontrar información sobre algunos de los escenarios de backup, restauración y recuperación que puede usar para lograr sus objetivos de protección de datos.

En la siguiente ilustración se muestra el contenido del tablespace:



En la ilustración, Tabespace1 tiene una tabla y dos archivos de base de datos asociados. Tabespace2 tiene dos tablas y un archivo de base de datos asociado.

En las siguientes tablas se describen algunos escenarios de backup, restauración y recuperación completos y parciales:

Ejemplos de operaciones de backup, restauración y recuperación completas

Backup completo	Restaurar	Recuperación
SnapManager realiza un backup del todo en la base de datos DB1, incluidos los archivos de datos, los registros de archivo y los ficheros de control.	La restauración completa con archivos de control SnapManager restaura todos los archivos de datos, espacios de tablas y archivos de control en el backup.	Puede especificar una de las opciones siguientes: • SCN: Introduzca un SCN, como 384641. • Fecha/hora: Introduzca una fecha y hora de la copia de seguridad, como 2005-11-25:19:06:22. • La última transacción realizada a la base de datos.
Restauración completa sin archivos de control SnapManager restaura todos los espacios de tablas y archivos de datos, sin los archivos de control.	Cuando se restauran los archivos de datos o los espacios de tablas con archivos de control, se especifica una de las siguientes opciones: • Espacios de tabla • Archivos de datos	SnapManager recupera los datos a la última transacción realizada a la base de datos.

Ejemplos de operaciones de backup, restauración y recuperación parciales

Copia de seguridad parcial	Restaurar	Recuperación

Es posible elegir una de las siguientes opciones: • Espacios de tabla Puede especificar Tablespaca1 y Tabespaca2 o sólo uno de ellos. • Archivos de datos Puede especificar los tres archivos de base de datos (TS1_1.dbf, TS1_2.dbf y TS2_1.dbf), dos archivos o un archivo. Independientemente de la opción que seleccione, el backup incluirá todos los archivos de control. Los archivos de registro de archivos se incluyen en el backup parcial si el perfil no está habilitado para crear los backups de los registros de archivos por separado.	La restauración completa de SnapManager restaura todos los archivos de datos, los espacios de tablas y los archivos de control especificados en el backup parcial.	SnapManager recupera los datos a la última transacción realizada a la instancia de la base de datos.

Restaure los archivos de datos o los espacios de tablas con los archivos de control SnapManager restaura uno de los siguientes elementos: • Todos los archivos de datos especificados • Todos los espacios de tablas especificados	Restaure los archivos de datos o los espacios de tablas sin los archivos de control SnapManager restaura uno de los siguientes elementos: • Espacios de tabla Especifique cualquiera de los espacios de tablas. SnapManager restaura solo los espacios de tablas especificados. Si la copia de seguridad contiene tablespace1, SnapManager sólo restaura ese tablespace. • Archivos de datos Especifique cualquiera de los archivos de la base de datos. SnapManager solo restaura los archivos de datos especificados. Si la copia de seguridad contiene archivos de base de datos (TS1_1.dbf y TS1_2.dbf), SnapManager sólo restaura esos archivos.	Únicamente restaure los archivos de control

Acerca del manejo de archivos de registro de archivo y archivos de control

SnapManager incluye los archivos de control y, opcionalmente, incluye los archivos de registro de archivo en cada backup. Los archivos de registro de archivo se usan para operaciones de recuperación.

La base de datos utiliza archivos de control para identificar nombres, ubicaciones y tamaños de los archivos de base de datos. SnapManager incluye los archivos de control en cada backup porque los archivos de control se utilizan en el proceso de restauración.

Se hace un seguimiento de los cambios en una base de datos mediante los redo logs en línea, que finalmente se archivan y se conocen como redo logs archivados (o archive logs). SnapManager (3.2 o posterior) permite realizar backups de los archivos de datos y los archivos de registro de archivos de forma independiente con diferentes retentions y frecuencias. SnapManager puede realizar backups únicamente de los registros de archivo o los backups combinados de archivos de datos y registros de archivos. SnapManager ofrece una gestión automatizada completa de los registros de archivos, y no requiere intervención manual para la recuperación de bases de datos. Además, permite la eliminación de registros de archivos de uno o más destinos de registros de archivos después de realizar el backup.

> Para ver qué tablespaces y archivos de datos se incluyen en una copia de seguridad, utilice el comando backup show o la ventana Backup Properties.

La siguiente tabla muestra cómo SnapManager gestiona los archivos de control y de registro de archivo

durante cada operación:

Tipo de operación	Archivos de control	Archivos de registro de archivo
Backup	Incluidas con cada backup	Se puede incluir con cada backup
Restaurar	Se pueden restaurar por separado o junto con los espacios de tablas o los ficheros de datos	Se puede usar para el proceso de recuperación

Qué es la programación de backups de base de datos

Puede programar, actualizar y supervisar las copias de seguridad de las bases de datos mediante la ficha Programación de la interfaz gráfica de usuario.

La siguiente tabla aborda algunas preguntas frecuentes sobre la programación:

Pregunta	Responda
¿Qué ocurre con los backups programados al reiniciarse el servidor de SnapManager?	Cuando se reinicia el servidor SnapManager, éste reinicia automáticamente todas las programaciones. Sin embargo, SnapManager no realiza seguimiento de ninguna incidencia perdida.

¿Qué sucede cuando se programan dos backups en dos bases de datos a la vez?	SnapManager inicia las operaciones de backup de uno en uno y luego permite que los backups se ejecuten en paralelo. Por ejemplo, si un administrador de bases de datos crea seis programaciones de backup diarias para seis perfiles de base de datos diferentes a las 00:00, los seis backups se ejecutan en paralelo. Si se programan varios backups en un único perfil de base de datos en un breve periodo de tiempo, el servidor SnapManager ejecutará solo la operación de backup con la duración de retención más larga. Antes de iniciar una operación de backup, SnapManager primero determina lo siguiente: • En los últimos 30 minutos, ¿ha creado otra programación correctamente un backup, con mayor retención, para el mismo perfil? • En los próximos 30 minutos, ¿intentará otra programación crear un backup, con mayor retención, para el mismo perfil? Si la respuesta a cualquiera de las dos preguntas es sí, SnapManager omite el backup. Por ejemplo, un administrador de bases de datos puede crear una programación diaria, semanal y mensual para un perfil de base de datos, y se prevé que todos los backups se realicen a las 1:00 a.m. En ese día del mes en el que se programan tres backups a la vez a las 1:00, SnapManager únicamente ejecutará la operación de backup en función de la programación mensual. La ventana de tiempo de 30 minutos se puede cambiar en un archivo de propiedades de SnapManager.
¿Con qué usuario se ejecuta la operación de backup?	La operación se ejecuta bajo el usuario que creó la programación. Sin embargo, es posible cambiarlo por su propio ID de usuario, si cuenta con credenciales válidas tanto para el perfil de base de datos como para el host. Por ejemplo, al iniciar las propiedades de copia de seguridad programada para la programación de copia de seguridad creada por Avida Davis, Stella Morrow puede seleccionar su ID de usuario en realizar esta operación como usuario para ejecutar la copia de seguridad programada.

¿Cómo interactúa el programador de SnapManager con el programador del sistema operativo nativo?	En el servidor SnapManager, no se pueden ver los backups programados a través del planificador nativo del sistema operativo. Por ejemplo, después de crear una copia de seguridad programada, no verá una nueva entrada en la ventana tareas programadas.

¿Qué sucede si los relojes de la interfaz gráfica de usuario y el servidor no están sincronizados?	Los relojes del cliente y del servidor no están sincronizados. Por lo tanto, puede programar una copia de seguridad en la que la hora de inicio esté en el futuro en el cliente pero en el pasado en el servidor. Para realizar backups periódicos, el servidor sigue cumpliendo la solicitud. Por ejemplo, si el servidor recibe una solicitud para realizar copias de seguridad cada hora comenzando un 01/30/08 a las 3:00 p.m. pero la hora actual es a las 3:30 p.m. ese día, el servidor realiza su primer backup a las 4:00 p.m. y continúa realizando backups cada hora. Sin embargo, durante los backups que solo se realizan una vez, el servidor gestiona la solicitud de la siguiente forma: • Si la hora de inicio está dentro de los últimos cinco minutos de la hora del servidor actual, SnapManager inicia de inmediato el backup. • Si la hora de inicio es superior a cinco minutos, SnapManager no inicia el backup. Por ejemplo, piense en el siguiente escenario: • El reloj del host de la interfaz gráfica está a tres minutos de distancia del tiempo real. • La hora actual en el cliente es 8:58 a.m. • Se programa un backup puntual a las 9:00 • Se programa otro backup que se realice una vez a las 8:30 Cuando el servidor recibe la primera solicitud, la hora en el servidor es 9:01 a.m. Aunque la hora de inicio del backup es anterior, SnapManager realiza el backup de forma inmediata. Cuando el servidor recibe la segunda solicitud, la hora de inicio del backup ha pasado más de cinco minutos. Recibirá un mensaje indicando que la solicitud de programa ha fallado porque la hora de inicio ha pasado. Puede cambiar el tiempo de cinco minutos en un archivo de propiedades de SnapManager.
¿Qué ocurre en los backups programados para un perfil cuando se elimina el perfil?	Cuando se elimina un perfil de base de datos, el servidor SnapManager elimina los backups programados definidos para ese perfil.

¿Cómo se comportan los backups programados durante el horario de verano o cuando se cambia la hora del servidor SnapManager?	Las programaciones de backups de SnapManager se ven afectadas por el horario de verano o al cambiar la hora del servidor SnapManager.
	
	Tenga en cuenta las siguientes implicaciones cuando cambie el tiempo del servidor SnapManager:
	
	• Después de activar la programación de copia de seguridad, si la hora del servidor SnapManager se reduce, la programación de copia de seguridad no se activa de nuevo.
	• Si la hora de verano comienza antes de la hora de inicio programada, las programaciones de backup se activan automáticamente.
	• Por ejemplo, si se encuentra en los Estados Unidos y se programan los backups cada hora a las 4:00 esto se debe producir cada 4 horas, se realizará un backup a las 4:00, 8:00, 12:00, 4:00, 8:00, Y medianoche los días antes y después de los ajustes de horario de verano en marzo y noviembre.
	• Tenga en cuenta lo siguiente si las copias de seguridad están programadas para las 2:30 a.m. todas las noches:
	  ◦ Cuando los relojes se atrasan una hora, ya que el backup se activa, el backup no se activa de nuevo.
	  ◦ Cuando los relojes se adelantan una hora, el backup se activa inmediatamente. Si se encuentra en los Estados Unidos y desea evitar este problema, debe programar las copias de seguridad para que comiencen fuera de las 2:00 a.m. a las 3:00 horas intervalo.

Creación de backups de la base de datos

Puede crear backups de bases de datos completas o de partes de bases de datos, incluidos espacios de tabla, archivos de datos o archivos de control.

Los administradores pueden opcionalmente registrar backups con Oracle RMAN, lo que facilita el uso de RMAN para restaurar y recuperar la base de datos con granularidades más finas como bloques.

Al definir el perfil, puede personalizar los nombres de las copias Snapshot creadas por backups de ese perfil. Por ejemplo, puede insertar una cadena de prefijo del NÚMERO DE SALTOS para indicar backups de operaciones altas.

Además de definir nombres únicos para las copias de Snapshot creadas por backups, también puede crear etiquetas únicas para los propios backups. Cuando se crea un backup, se recomienda proporcionar un nombre para el backup de forma que se cuente con un método sencillo para identificarlo con el parámetro

-label. Este nombre debe ser único para todos los backups creados dentro de un perfil determinado. El nombre puede contener letras, números, guiones bajos (_) y guiones (-). No puede comenzar con un guión. Las etiquetas distinguen mayúsculas de minúsculas. Puede incluir información como variables de entorno del sistema operativo, fecha del sistema y tipo de backup.

Si no proporciona una etiqueta, SnapManager crea un nombre de etiqueta predeterminado en la forma scope_mode_datestring, donde el ámbito está completo o parcial y el modo está sin conexión, en línea o automático (la letra c para frío, h para caliente o a para automático).

Desde SnapManager 3.4, puede proporcionar su propia etiqueta de backup reemplazando la etiqueta de backup predeterminada que creó SnapManager. Debe configurar el valor del parámetro override.default.backup.pattern en TRUE y especificar la nueva etiqueta de backup en el parámetro new.default.backup.pattern. El patrón de etiqueta de backup puede contener palabras clave como el nombre de la base de datos, el nombre del perfil, el ámbito, el modo y el nombre de host, que deben separarse con el guión bajo. Por ejemplo, new.default.backup.pattern=dbname_profile_hostname_scope_mode.

La Marca de hora se incluirá automáticamente al final de la etiqueta generada.

Al introducir un comentario, puede incluir espacios y caracteres especiales. Por el contrario, cuando introduzca una etiqueta, no incluya espacios ni caracteres especiales.

Para cada backup, SnapManager genera automáticamente un GUID, que es una cadena HEXADECIMAL de 32 caracteres. Para determinar el GUID, debe ejecutar el comando backup list con la opción -verbose.

Es posible crear un backup completo de una base de datos mientras está en línea o sin conexión. Para permitir que SnapManager gestione el backup de una base de datos independientemente de si está en línea o sin conexión, debe utilizar la opción -auto.

Al crear un backup, si se habilitó la eliminación y se habilitó la notificación de resumen en el perfil, se activan dos correos electrónicos independientes. Un correo electrónico es para la operación de backup y el otro para la eliminación. Es posible correlacionar estos correos electrónicos comparando el nombre de la copia de seguridad y el ID de copia de seguridad incluidos en estos correos electrónicos.

Es posible crear un backup en frío cuando la base de datos está en estado de apagado. Si la base de datos está en estado montado, cambie a estado de apagado y realice el backup sin conexión (backup en frío).

SnapManager (3.2 o posterior) permite realizar un backup de los archivos de registro de archivos independientemente de los archivos de datos, lo que permite gestionar los archivos de registro de archivos de forma eficiente.

Para crear los backups de registros de archivos por separado, debe crear un nuevo perfil o actualizar el perfil existente para separar los backups de los registros de archivos con la opción -separate-archivvelog-backups. Con el perfil, es posible realizar las siguientes operaciones de SnapManager:

- Cree un backup de registro de archivos.
- Eliminar un backup de registro de archivos.
- Montar un backup de registro de archivos.
- Liberar un backup de registro de archivo.

Las opciones de copia de seguridad varían en función de la configuración del perfil:

- Si se utiliza un perfil que no está separado para realizar backups de registros de archivos de forma independiente, se puede hacer lo siguiente:

- Cree un backup completo.
- Crear un backup parcial.
- Especifique los destinos de registros de archivos que se incluirán en el backup para los archivos de registro de archivos.
- Especifique los destinos de registro de archivos que se excluirán de la copia de seguridad.
- Especifique las opciones de eliminación para eliminar los archivos de registro de archivos de los destinos de registro de archivos.

- El uso de un perfil separado para tomar backups de registros de archivos permite hacer lo siguiente:
  - Cree una copia de seguridad sólo de archivos de datos.
  - Cree un backup solo de archivado.
  - Durante la creación de un backup solo de archivos de datos, incluya el backup de registro de archivos junto con el backup en línea de solo los archivos de datos para el clonado.

    Si ha incluido copias de seguridad de registros de archivos junto con archivos de datos en la página **Configuración de perfiles** del asistente **creación de perfiles** de la interfaz gráfica de usuario de SnapManager, Y si no ha seleccionado la opción **Archivelogs** en el asistente **creación de copia de seguridad**, SnapManager siempre crea la copia de seguridad del registro de archivos junto con los archivos de datos para todas las copias de seguridad en línea.

    En tal situación, en la CLI de SnapManager, puede tener en cuenta todos los destinos de los registros de archivos para el backup, excepto los destinos de exclusión especificados en el archivo de configuración SnapManager. Pero no puede eliminar estos archivos de registro de archivos. Sin embargo, puede seguir utilizando la opción -archivovelogs para especificar el destino del archivo de registro de archivos y hacer un uso de los archivos de registro de archivos desde la interfaz de línea de comandos de SnapManager.

    Si crea el backup con la opción -auto y especifica la opción --archivelogs, SnapManager crea un backup en línea o sin conexión según el estado actual del backup.

    - SnapManager crea un backup sin conexión cuando la base de datos está sin conexión y no incluye los archivos de registro de archivos en el backup.
    - SnapManager crea un backup en línea incluidos los archivos de registro de archivos cuando la base de datos está en línea.
  - Mientras se crea el backup de solo archivado:
    - Especifique el destino de registro de archivos que se realizará el backup junto con el backup solo de archivmogs
    - Especifique los destinos de registro de archivos que se excluirán del backup solo de registros de archivo
    - Especifique las opciones de eliminación para eliminar los archivos de registro de archivos de los destinos de registro de archivos
- **Escenarios no admitidos**
  - No puede crear el backup solo de archivado junto con un backup de solo archivos de datos sin conexión.
  - No se pueden reducir los archivos de registro de archivos cuando no se realiza el backup de los archivos de registro de archivos.
  - No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos.

Si especifica la ubicación del registro de archivos en el área de recuperación flash, debe asegurarse de especificar también la ubicación del registro de archivos en el parámetro archive_log_dest.

> Al crear backups de los registros de archivos, debe introducir las rutas de destino completas de los registros de archivos dentro de comillas dobles y las rutas de destino separadas por comas. El separador de ruta debe ser dado como dos barras invertidas (\\) en lugar de una.

Al especificar la etiqueta para la copia de seguridad de archivos de datos en línea con la copia de seguridad de archivos de archivo incluida, se aplica la etiqueta para la copia de seguridad de archivos de datos, y la copia de seguridad del registro de archivo se adjuntará con el sufijo (_logs). Este sufijo puede configurarse cambiando el parámetro suffix.backup.label.with.logs en el archivo de configuración de SnapManager.

Por ejemplo, puede especificar el valor como suffix.backup.label.with.logs=Arc para que el valor predeterminado _logs cambie a _Arc.

Si no se especificaron destinos de registro de archivos para su inclusión en el backup, SnapManager incluye todos los destinos de registro de archivos configurados en la base de datos.

Si falta algún archivo de registro de archivo en alguno de los destinos, SnapManager omite todos estos archivos de registro de archivos creados antes de los archivos de registro de archivos que faltan aunque estos archivos estén disponibles en otro destino de registro de archivos.

Al crear backups de registros de archivos, es necesario especificar los destinos de archivos de registro de archivos que se incluirán en el backup. Además, puede configurar el parámetro Configuration para incluir los archivos de registro de archivos siempre más allá de los archivos faltantes en el backup.

> De forma predeterminada, este parámetro de configuración se establece en TRUE para incluir todos los archivos de registro de archivos, más allá de los archivos que faltan. Si utiliza sus propios scripts de eliminación de registros de archivos o eliminación manual de archivos de registro de archivos de los destinos de registro de archivos, puede deshabilitar este parámetro, para que SnapManager pueda omitir los archivos de registro de archivos y continuar con el backup.

SnapManager no admite las siguientes operaciones SnapManager para backups de registros de archivos:

- Clone el backup de registros de archivos
- Restaurar el backup de registros de archivos
- Verificar el backup de registros de archivos

SnapManager también admite la copia de seguridad de los archivos de registro de archivos desde los destinos de área de recuperación flash.

1. Introduzca el siguiente comando: smo backup create -profile_name {[-full {-online | -offline | -auto} [-retain {-hora | -diario | -semanal | -mensual | -ilimitado}] [-verify] | [-data [-filesfiles [ficheros] | [-tablespaces [-commentation]]] [-datalabellabel] | -retain] | -compointing] [-backup-destinpath1 [,[path2]]] [-exclude-destinpath1 [,path2]]] [-prunogs {-all | -untilSCNuntilSCN | -until-date aaaa-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}]-pruni] [-pruni]-pruni]-pruni]

Si desea…	Realice lo siguiente…

Especifique si desea realizar una copia de seguridad de una base de datos en línea o sin conexión, en lugar de permitir que SnapManager controle si está en línea o sin conexión	Specify -offline para realizar un backup de la base de datos sin conexión. Specify -online para realizar un backup de la base de datos en línea. + Si utiliza estas opciones, no puede utilizar la opción -auto.
Especifique si desea que SnapManager gestione la copia de seguridad de una base de datos independientemente de si está en línea o sin conexión	Especifique la opción -auto. Si utiliza esta opción, no podrá utilizar la opción --offline o -online.

Especifique si desea realizar una copia de seguridad parcial de archivos específicos	`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.`
	`+ ejemplo para crear una copia de seguridad parcial del archivo de datos en Windows`
	
	+
	
	`smo backup create -profile nosep -data -files "J:\\mnt\\user\\user.dbf" -online -label partial_datafile_backup -verbose`

Especifique si desea realizar una copia de seguridad parcial de tablespaces específicos	`Specify the -data-tablespaces option and then list the tablespaces, separated by commas. For example, use ts1, ts2, and ts3 after the option.`
	+ SnapManager permite realizar backup de espacios de tablas de solo lectura. Al crear el backup, SnapManager cambia los espacios de tabla de solo lectura a lectura y escritura. Después de crear el backup, los espacios de tabla se modifican a modo de solo lectura.
	
	+ ejemplo para crear una copia de seguridad de tablespace parcial
	
	+
	
	`smo backup create -profile nosep -data -tablespaces tb2 -online -label partial_tablespace_bkup -verbose`

Especifique si desea crear una etiqueta única para cada copia de seguridad en el siguiente formato: 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`

Especifique si desea crear una copia de seguridad de los archivos de registro de archivos por separado de los archivos de datos	`Specify the following options and variables:`
	`** -archivvelogs crea una copia de seguridad de los archivos de registro de archivo.`
	`** -backup-dest especifica los destinos de archivos de registro de archivos que se incluirán en el backup.`
	`** -exclude-dest especifica los destinos de registro de archivos que se van a excluir.`
	`** -label especifica la etiqueta para el backup del archivo de registro de archivos. *Nota:* debe proporcionar la opción -backup-dest o la opción -exclude -dest.`
	
	+ Si se proporcionan ambas opciones junto con la copia de seguridad, se muestra un mensaje de error que ha especificado una opción de copia de seguridad no válida. Especifique una de las opciones: -Backup-dest o exclude-dest.
	
	+ Ejemplo de creación de backups de archivos de registro de archivos por separado en Windows
	
	+
	
	`smo backup create -profile nosep -archivelogs -backup-dest "J:\\mnt\\archive_dest_2\\" -label archivelog_backup -verbose`

Especifique si desea crear una copia de seguridad de archivos de datos y archivos de registro de archivos juntos	`Specify the following options and variables:`
	`** -data option para especificar los archivos de datos.`
	`** -archivelogs opción para especificar los archivos de registro de archivos. Ejemplo para realizar copias de seguridad de archivos de datos y archivos de registro de archivo juntos en Windows`
	
	+
	
	`smo backup create -profile nosep -data -online -archivelogs -backup-dest "J:\\mnt\\archive_dest_2\\" -label data_arch_backup -verbose`

Especifique si desea eliminar los archivos de registro de archivos mientras crea una copia de seguridad	`Specify the following options and variables:`
	`** -prunelogs especifica que se eliminen los archivos de registro de archivos de los destinos de registro de archivos.`
	
	+ * **-all especifica que se eliminen todos los archivos de registro de archivos de los destinos de registro de archivos.** * -Until-scnuntil-scn especifica que se eliminen los archivos de registro de archivos hasta un SCN especificado. *** -Until -dateyyyy-MM-dd:HH:mm:ss especifica que se eliminen los archivos de registro de archivos hasta el período de tiempo especificado.** * la opción -before especifica la eliminación de los archivos de registro de archivos antes del período de tiempo especificado (días, meses, semanas, horas). ***** -prune-destprune_dest1,[prune_dest2 especifica que se eliminen los archivos de registro de archivo de los destinos de registro de archivo mientras se crea la copia de seguridad. **Nota:** no puede pinar los archivos de registro de archivos cuando el área de recuperación de Flash (FRA) está activada para archivos de registro de archivos.
	
	+ Ejemplo para eliminar todos los archivos de registro de archivos mientras se crea una copia de seguridad en Windows
	
	+
	
	+
	
	+
	
	`smo backup create -profile nosep -archivelogs -label archive_prunebackup1 -backup-dest "E:\\oracle\\MDV\\oraarch\\MDVarch,J:\\ " -prunelogs -all -prune-dest "E:\\oracle\\MDV\\oraarch\\MDVarch,J:\\" -verbose`

Especifique si desea añadir un comentario sobre la copia de seguridad	Especifique -comment seguido de la cadena de descripción.

Especifique si desea forzar la base de datos al estado que ha especificado para realizar la copia de seguridad, independientemente del estado en el que se encuentre	Especifique la opción -force.
Especifique si desea verificar la copia de seguridad al mismo tiempo que la crea	Especifique la opción -Verify.
Especifique si desea recopilar los archivos de volcado después de la operación de copia de seguridad de la base de datos	Especifique la opción -dump al final del comando de creación de backup.

Ejemplo

```
smo backup create -profile targetdb1_prof1 -full -online -force  -verify
```

Información relacionada

Nomenclatura de copias Snapshot

Crear scripts de tareas previas, tareas posteriores y directivas

Creación de scripts de tareas

Almacenamiento de los scripts de tareas

El comando smo backup create

Creación o actualización de los scripts posteriores

Eliminar archivos de registro de archivos

Puede reducir los archivos de registro de archivos desde las ubicaciones del registro de archivos mientras crea una copia de seguridad.

- La operación de backup actual debe realizar un backup de los archivos de registro de archivos.

  Si se especifica la eliminación junto con otros backups que no contienen archivos de registro de archivos, no se reducen los archivos de registro de archivos.

- La base de datos debe estar en el estado montado.

  Si la base de datos no está en estado montado, introduzca la opción -force junto con el comando de backup.

Al realizar una operación de backup, se puede especificar lo siguiente:

- Ámbito de la eliminación:
  - Elimine todos los archivos de registro de archivos.

- Elimine los archivos de registro de archivos hasta que el SCN especificado.
- Elimine los archivos de registro de archivos hasta la hora especificada.
- Elimine los archivos de registro de archivos antes del período de tiempo especificado.

- Destino desde el que se deben quitar los archivos de registro de archivos.

> Aunque se produzca un error al eliminar el archivo de registro de archivos en un destino, SnapManager continúa depurando los archivos de registro de archivos de los otros destinos.

Antes de eliminar los archivos de registro de archivos, SnapManager verifica lo siguiente:

- Se realiza un backup de los archivos de registro de archivo al menos una vez.
- Los archivos de registro de archivo se envían a la base de datos Oracle Dataguard Standby, si los hubiera.
- El proceso de captura de Oracle Streams captura los archivos de registro de archivo, si los hay.

Si se realiza un backup de los archivos de registro de archivos, se envían al estado de espera y se capturan mediante el proceso de captura, SnapManager elimina todos los archivos de registro de archivos en una sola ejecución. Sin embargo, si hay archivos de registro de archivos que no se incluyen en un backup, que no se envían a en espera o que no están capturados por el proceso de captura, SnapManager elimina los archivos de registro de archivos uno por uno. La eliminación de archivos de registros de archivos en una sola ejecución es más rápida que la eliminación de registros de archivos uno por uno.

SnapManager también puede agrupar los archivos de registro de archivos y eliminarlos por lotes. Cada lote tendrá un máximo de 998 archivos. Este valor se puede configurar por debajo de 998 utilizando el parámetro de configuración Maximum.archivvelog.files.torune.atATime en el archivo smo.config.

SnapManager utiliza los comandos de Oracle Recovery Manager (RMAN) para eliminar los archivos de registro de archivo. Sin embargo, SnapManager no se integra con las políticas de retención y de eliminación de RMAN.

> Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.

SnapManager no admite la eliminación de archivos de registro de archivos en las siguientes situaciones:

- Los archivos de registro de archivo se encuentran en el área de recuperación de flash.
- Los archivos de registro de archivo se encuentran en la base de datos en espera.
- SnapManager y RMAN gestionan los archivos de registro de archivo.

  a. Introduzca el siguiente comando: smo backup create -profile_name {[-full {-online | -offline | -auto} [-retain {-hora | [-diario | -semanal | -mensual | -unlimited}] [-verify] | [-data [-filesprespresprespresnaces [ficheros] | [-destellabel] [-stockespaces] -retain] | -backup] [-those [,[pat2]]] [-exclude-destinpath1 [,path2]]] [-podelogs {-all | -untilSCNuntilSCN | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours} -prune-destprune] [desprunce]]-prunce]

Si desea…	Realice lo siguiente…

Prune archive log files	Especifique las siguientes opciones: • -prunelogs especifica la eliminación de los archivos de registro de archivos mientras se crea un backup. ◦ -all especifica la eliminación de todos los archivos de registro de archivos. ◦ -UntilSCN especifica la eliminación de los archivos de registro de archivos hasta el SCN especificado. ◦ -until-date especifica la eliminación de los registros de archivo incluyendo la fecha y hora especificadas. ◦ -antes de {-meses
-días	-semanas
-hours} especifica la eliminación de los archivos de registro de archivos antes del periodo de tiempo especificado.	• Incluir el destino desde donde se van a quitar los archivos de registro *

Consolidación de backups de registros de archivos

SnapManager consolida los backups de solo archivado cada vez que realiza un backup liberando únicamente los backups duplicados de archivvelog. La consolidación está habilitada de forma predeterminada.

SnapManager identifica los backups solo de archivado que tienen archivos de registro de archivos en otros backups y los libera para mantener la cantidad mínima de backups de solo archivado con archivos de registro únicos.

Si la consolidación libera los backups de solo archivado, estos backups se eliminan según la duración de la retención del registro de archivos.

Cuando la base de datos se encuentra en el estado shutdown o nomount durante la consolidación del registro de archivo, SnapManager cambia la base de datos al estado Mount.

Si se produce un error en la copia de seguridad o la eliminación de archivos de registro de archivos, no se realizará la consolidación. La consolidación de backups de solo archivovelog se sigue solo después de backups correctos y de operaciones de eliminación correctas.

1. Para permitir la consolidación de los backups de solo archivado, modifique la consolidación de los parámetros de configuración y establezca el valor como TRUE en el archivo de configuración SnapManager (smo.config).

   Una vez configurado el parámetro, se consolidan los backups de solo archivado.

   Si el backup de solo archivado creado recientemente contiene los mismos archivos de registro de archivos en cualquiera de los backups de solo archivado anteriores, se liberan los backups de solo registros de archivos anteriores.

SnapManager no consolida el backup de registros de archivos realizado junto con el backup de archivos de datos. SnapManager consolida el backup de solo archivado.

SnapManager consolida los backups de registros de archivos, incluso cuando el usuario elimina manualmente los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados y pueden incluirse el backup.

2. Para deshabilitar la consolidación de los backups de registros de archivo, modifique la consolidación de los parámetros de configuración y establezca el valor como FALSE en el archivo de configuración de SnapManager (smo.config).

Programar la eliminación del archivo de registro de archivos

Cuando se crea un backup, es posible programar la eliminación de los archivos de registro de archivos para que se produzca en un momento determinado.

SnapManager permite reducir periódicamente los archivos de registro de archivos desde el sistema de archivos activo.

1. Introduzca el siguiente comando: Programación de smo create -profile_name {[-full {-online | -offline | -auto}[-retain [-horaria | -diario | -semanal | -mensual | -ilimitado] [-verify] | [-data [-filesfiles [ficheros] | [-tablespaces [-destapaces]]]] {-online | -patheld] [-destapparkmo.com]]] [-pathways]]]]-1] [-1]]-achut]-pathways] [-1] [-1]]]] [-prunelogs{-all | -untilSCNuntillschedule | -before {-dateyyyy-MM-dd HH:mm:ss | -months | -weeksweeks | -daysdays | -hourshours} -prune-destprune_dest1,,prune_dest2] -time-schedule [<yyyy-MM-dd HH:mm> -time-time-time-time-time-time-time-time-get_stunit]

Si desea…	Realice lo siguiente…
Programar la eliminación de archivos de registro de archivos	Especifique las siguientes opciones: • -prunelogs para programar la eliminación de los archivos de registro de archivo • -prune-dest para depurar archivos de registro de archivos desde los destinos de registro de archivos
Incluya un nombre para el horario	Especifique la opción -schedule-name.
Programar la eliminación de archivos de registro de archivos en un intervalo de tiempo específico	Especifique la opción INTERVAL e indique si los archivos log de archivo deben recordarse en función de las siguientes clases de intervalo: • -cada hora • - diariamente • -semanal • -mensual • -untimeonly

Agregar un comentario sobre la operación de horario	Especifique la opción -schedule-comment seguida de la cadena de descripción.
Especifique la hora de inicio de la operación de programación	Especifique la opción -start-time en el formato yyyy-mm-dd hh:mm.

Qué es AutoSupport

La función AutoSupport permite que el servidor SnapManager envíe mensajes de AutoSupport al sistema de almacenamiento una vez completada la operación de backup.

SnapManager envía mensajes de AutoSupport solo para las operaciones de backup correctas.

Puede habilitar o deshabilitar AutoSupport asignando los siguientes valores al parámetro de configuración auto_support.on en el archivo de configuración de smo.config:

- TRUE - habilita AutoSupport
- FALSE - deshabilita AutoSupport

De manera predeterminada, AutoSupport se habilita en SnapManager.

Información relacionada

Añadir sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager

Habilitar AutoSupport en SnapManager

Deshabilitar AutoSupport en SnapManager

Añadir sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager

Debe añadir los sistemas de almacenamiento operativos en Clustered Data ONTAP al host del servidor de SnapManager para habilitar AutoSupport. En SnapManager 3.3 y versiones anteriores, AutoSupport solo era compatible con sistemas de almacenamiento que funcionaban en 7-Mode.

1. Añada una máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) y una SVM que opera en Clustered Data ONTAP al host del servidor de SnapManager: Sdcli Transport_protocol set -f AdminVServer_name o vserver_NAME -type HTTP -user admin

   Escriba el siguiente comando: Se muestra el mensaje.

2. Introduzca la contraseña que proporcionó al crear la SVM.

   Después de ejecutar el comando correctamente, se ha establecido el nuevo protocolo de transporte. aparece el mensaje.

Habilitar AutoSupport en SnapManager

Debe habilitar AutoSupport, de modo que los sistemas de almacenamiento reciban mensajes del servidor SnapManager para cada operación de backup realizada correctamente.

AutoSupport se puede habilitar de dos formas:

- De forma predeterminada, la nueva instalación de SnapManager no contiene el parámetro auto_support.on en el archivo de configuración smo.config. Esto implica que AutoSupport está habilitado.
- Puede configurar manualmente el parámetro auto_support.on.
  a. Detenga el servidor SnapManager.
  b. En el archivo de configuración smo.config, establezca el valor del parámetro auto_support.on en TRUE.

     auto_support.on=TRUE

  c. Reinicie el servidor SnapManager.

Deshabilitar AutoSupport en SnapManager

Debe deshabilitar AutoSupport si no desea que el sistema de almacenamiento reciba mensajes del servidor SnapManager para cada operación de backup exitosa.

De manera predeterminada, AutoSupport se habilita si el archivo de configuración no contiene el parámetro auto_support.on. En este escenario, debe agregar el parámetro auto_support.on en el archivo de configuración y establecer el valor EN FALSE.

1. Detenga el servidor SnapManager.
2. En el archivo de configuración smo.config, establezca el valor del parámetro auto_support.on en FALSE.

   auto_support.on=FALSE

3. Reinicie el servidor SnapManager.

Verificación de los backups de las bases de datos

Es posible utilizar el comando backup verify para verificar que los bloques del backup de la base de datos no están dañados. La operación Verify invoca la utilidad Oracle Database Verify para cada archivo de datos de la copia de seguridad.

SnapManager permite realizar la operación de verificación cuando lo desee, tanto para usted como para los usuarios del sistema. Es posible realizar la verificación inmediatamente después de crear el backup. Debe especificar el perfil que contiene el backup y la etiqueta o el ID del backup creado.

> Se produce un error en la operación de verificación de backups en un entorno de Windows si se utiliza SnapManager 3.0 y Oracle Database 11.1.0.7. Se debe utilizar la base de datos de Oracle 11.2.0.1 o posterior.

Es posible especificar -dump para recoger los archivos de volcado después de la operación de verificación de backup.

1. Introduzca el siguiente comando: smo backup verify -profile profile profile_name [-label label label | -idid] [-force] [-dump] [-quiet | -verbose]

Información relacionada

El comando smo backup verify

Cambiar la política de retención de backups

Puede cambiar las propiedades de un backup para que sea elegible o inelegible para su eliminación de acuerdo con la política de retención.

Al crear un backup, se puede establecer su política de retención. Posteriormente, se puede optar por conservar el backup durante un período más largo del que permite la política de retención o especificar que ya no es necesario el backup y desea que la política de retención lo gestione.

Información relacionada

El comando de actualización de backup de smo

Retención permanente de backups

Puede especificar que una copia de seguridad no sea elegible para su eliminación por parte de la política de retención, con el fin de conservar el backup de forma indefinida.

1. Para especificar que una copia de seguridad se conserve de forma ilimitada, introduzca este comando:actualización de copia de seguridad de smo -profileprofile_name {-labellabel [data | -archivvelogs] | -idid} -retain -Unlimited

Información relacionada

El comando de actualización de backup de smo

Asignar backups con una clase de retención específica

Los administradores de bases de datos pueden asignar una clase de retención específica por hora, día, semana o mes a los backups. La asignación de una clase de retención específica hace que los backups realizados bajo este cambio sean aptos para su eliminación.

1. Para asignar una clase de retención de copia de seguridad específica, introduzca este comando:SMO backup update -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | all} -retain [-Hourly | -Daily | -Weekly | -Monthly]

Cambiar el comportamiento predeterminado de la política de retención

Cuando caduca un backup según la política de retención, SnapManager determina si se elimina el backup según la configuración de retención. La eliminación de copias de seguridad es el comportamiento predeterminado. Puede cambiar este comportamiento

predeterminado y liberar en su lugar las copias de seguridad no protegidas.

De forma predeterminada, Snap Manager elimina la copia de seguridad cuando caducan.

1. Acceda a la siguiente ubicación predeterminada:

   ubicación\propiedades\smo.config predeterminada de la instalación de smo

2. Edite el archivo smo.config.
3. Establezca la propiedad retain.always FreeExpiredbackups en el archivo smo.config en true.

   Por ejemplo, retain.always FreeExpiredbackups = true

Información relacionada

El comando de actualización de backup de smo

Liberar o eliminar backups exentos de la política de retención

Los backups con clase de retención "ilimitada" no se pueden eliminar ni liberar directamente. Para eliminar o liberar estos backups, primero se debe asignar otra clase de retención, como por ejemplo cada hora, día, semana o mes. Para eliminar o liberar una copia de seguridad que esté exenta de la política de retención, primero debe actualizar la copia de seguridad para que sea elegible para su eliminación o su liberación.

1. Para actualizar la copia de seguridad para que pueda ser eliminada por la política de retención, introduzca este comando: Actualización de copia de seguridad de smo -profileprofile_name {-labellabel [data | -archivvelogs] | -idid} -retain [-hora | -diaria | -semanal | -mensual]
2. Después de actualizar el backup de modo que sea apto para su eliminación, puede eliminar el backup o liberar recursos de backup.
   - Para eliminar la copia de seguridad, introduzca este comando: smo backup delete -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | -all}
   - Para liberar los recursos de copia de seguridad, en lugar de eliminar la copia de seguridad, introduzca este comando:smo backup free -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | -all} [-force] [-dump] [-quiet | -verbose]

Información relacionada

El comando de actualización de backup de smo

Ver una lista de backups

Puede comprobar qué backups se han creado para un perfil y su estado de backup mediante el comando smo backup list. Para cada perfil, el comando muestra primero la información sobre el backup más reciente y, a continuación, continúa hasta que se muestra la información de todos los backups.

1. Introduzca el siguiente comando: smo backup list -profileprofile_name [-delimitercharacter] [data | -archivvelogs] [-quiet | -verbose]

Información relacionada

El comando smo backup list

Ver los detalles de backup

Puede ver la información detallada sobre un backup concreto de un perfil mediante el comando smo backup show.

El comando smo backup show muestra la siguiente información de cada backup:

- El ID de la copia de seguridad
- Si la copia de seguridad se ha realizado correctamente o ha fallado
- Alcance de backup (completo, parcial, en línea o sin conexión)
- Modo de backup
- Estado de montaje
- La etiqueta de backup
- Comentar
- La fecha y la hora en que se inició y finalizó la operación
- Información sobre si se verificó el backup
- La clase de retención de copias de seguridad
- La base de datos y el nombre de host
- El número de cambio de sistema de punto de comprobación (SCN)
- El SCN de backup final (solo para backups en línea)
- Los espacios de tablas y los archivos de datos de la base de datos de la que se realizó un backup
- Los archivos de control de la base de datos de la que se realizó un backup
- Los registros de archivos de la base de datos de la que se realizó un backup
- El sistema de almacenamiento y los volúmenes donde se encuentran los archivos
- Las copias Snapshot realizadas y su ubicación
- El estado de los recursos de almacenamiento principales
- El estado de la protección de backup
- Modo de backup

Si especifica la opción -verbose, se muestra la siguiente información adicional:

- Los clones del backup, si los hay
- Información de verificación
- Si se monta el backup, SnapManager muestra los puntos de montaje que están en uso

Para el backup de archivos de registro de archivos, se muestra la misma información que la del otro backup de base de datos excepto la siguiente información:

- SCN de punto de comprobación

- SCN de backup final
- Tablespace
- Archivos de control

Sin embargo, el backup del archivo de registro de archivos contiene la siguiente información adicional:

- El primer número de cambio del backup
- El siguiente número de cambio del backup
- Número de rosca
- Restablecer ID de registros
- Encarnación
- Nombre de archivo de registro
  a. Introduzca el siguiente comando:smo backup show -profileprofile_name {-labellabel [data | -archivvelogs] | -id [-quiet | -verbose]

Información relacionada

El comando smo backup show

Montar backups

SnapManager se encarga automáticamente del montaje de un backup para que el host esté disponible. También es posible montar backups en situaciones en las que se utilice una herramienta externa, como Oracle Recovery Manager (RMAN), para acceder a los archivos de la copia de seguridad.

Si utiliza RMAN, debe utilizar la operación de montaje para cambiar el estado de un backup (que permite el acceso) y la operación de desmontaje para cambiar el estado de un backup (que quita el acceso).

El comando smo backup Mount muestra una lista de rutas donde se han montado las copias Snapshot consistentes en el backup.

> Opcionalmente, es posible recoger los archivos de volcado después de una operación de montaje de backup exitosa o con errores.

1. Para montar una copia de seguridad, introduzca el siguiente comando: smo backup Mount -profile profile_name {labellabel [data | -archivvelogs] | -idid} [-host-dump] [-quiet | -verbose]

Información relacionada

El comando de montaje de backup de smo

Desmontaje de backups

SnapManager desmonta automáticamente el backup para que no esté disponible para el servidor host. SnapManager también permite desmontar si se utiliza una herramienta externa, como Oracle Recovery Manager (RMAN), para acceder a los archivos de la copia de seguridad y para cambiar el estado del backup para quitar el acceso.

Otra opción es recoger los archivos de volcado después de una operación de backup realizó una operación de desmontaje correcta o con errores.

1. Introduzca el siguiente comando: smo backup unmount -profile profile_name {labellabel [data | -archivvelogs] | -idid} [-quiet | -verbose] -dump-force-verbose

Información relacionada

El comando de desmontaje del backup de smo

Liberando backups

Es posible liberar backups, lo que elimina las copias Snapshot sin eliminar los metadatos de los backups. Esta función libera el espacio ocupado por la copia de seguridad. Puede utilizar el comando libre del backup de smo para liberar los backups.

Para que un backup pueda ser apto para liberar, debe asegurarse de lo siguiente:

- La copia de seguridad se ha realizado correctamente
- La copia de seguridad no se va a montar
- El backup no tiene clones
- El backup no se conservará mediante una política de retención ilimitada
- El backup no se ha liberado todavía

Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de backup libre exitosa o con errores.

1. Introduzca el siguiente comando: smo backup free -profileprofile_name {-labellabel [data | -archivvelogs] | -idid | -all} -force [-dump] [-quiet] [-force]

Información relacionada

El comando libre de backup de smo

Eliminar backups

Debe eliminar backups cuando ya no los necesite, lo que libera el espacio que estos backups ocupan. Si elimina los backups, reducirá la posibilidad de alcanzar el límite de 255 copias snapshot por volumen.

- Debe asegurarse de que el backup no se haya usado para crear un clon.

Puede eliminar backups retenidos de forma ilimitada sin cambiar la clase de retención.

Opcionalmente, es posible recoger los archivos de volcado después de la operación de eliminación de backup exitosa o con errores.

Si desea eliminar los backups de registros de archivos, debe comprobar la duración de retención establecida para el backup de registros de archivos. Si el backup de registros de archivos se encuentra dentro de la duración de retención y se requieren archivos de registro de archivos para la recuperación de una base de datos restaurada, no se puede eliminar el backup de registros de archivos.

1. Para verificar que las operaciones se han completado, introduzca el siguiente comando: smo operation list -profileprofile_name-quiet-verbose
2. Para eliminar una copia de seguridad, introduzca el siguiente comando:copia de seguridad de smo delete -profile profile_name [-label label label label [data | -archivvelogs] | -idid | -all] [-force] [-dump] [-quiet | -verbose]

   Utilice la opción -force para forzar la eliminación del backup. Forzar la eliminación de un backup que tenga operaciones incompletas podría dejar el backup en estado incoherente.

Programación de backups de bases de datos

SnapManager (3.2 o posterior) para Oracle permite programar backups de bases de datos de forma regular durante las horas de menor actividad para mantener un alto rendimiento. Para programar un backup, puede crear un perfil, que incluya la información de la base de datos y la política de retención, y luego establecer programaciones para el backup.

> Debe programar los backups como administrador. Si intenta programar los backups como usuario no existente, SnapManager muestra un mensaje de error: Invalid user: username: No puede crear un backup de programación para un usuario determinado

A continuación, se muestran algunas de las tareas relacionadas con la programación:

- Programar un backup de base de datos para que se realice por hora, día, semana, mes o una sola vez.
- Ver una lista de los backups programados asociados con un perfil.
- Actualizar una copia de seguridad programada.
- Suspender temporalmente una programación.
- Reanude la programación suspendida.
- Eliminar una programación.

> La casilla de verificación **operación del menú Ejecutar ahora** está desactivada cuando se está ejecutando una copia de seguridad programada para esa programación.

Creando programaciones de backup

Es posible programar un backup en el momento y la frecuencia que sean adecuados para sus datos y entorno.

En SnapManager 3.2 para Oracle, es posible programar los backups de los archivos de registro de archivos por separado. Sin embargo, debe utilizar el perfil que ha creado para separar los archivos de registro de archivos.

Si programó los backups de los archivos de datos y los archivos de registro de archivos al mismo tiempo, SnapManager creará primero el backup de los archivos de datos.

Si selecciona el intervalo de programación como -onetimeonly, todas las opciones de eliminación estarán disponibles. Si selecciona un intervalo de programación distinto de -onetime only, no se admiten las opciones de eliminación -until-SCN y -until-date y se muestra el siguiente mensaje de error: La opción de eliminación

del registro de archivado especificada, -until-scn o -until-date para el intervalo por hora de programación no es válida. Especifique la opción -onetimeonly para el intervalo de programación o pine los registros de archivo utilizando cualquiera de las opciones all, o -before {-months | -days | -weeks| -hours}.

Cuando se produce una conmutación al nodo de respaldo en los entornos de Microsoft Windows Server Failover Cluster (WSFC) y Microsoft Cluster Server (MSCS), debe reiniciar el servidor SnapManager para Oracle de modo que la dirección del servicio (virtual) se asigne al host activo y las programaciones de SnapManager se ajusten al host SnapManager activo.

> Si existe el mismo perfil y nombre de programación en otro repositorio, no se inicia la operación de programación de backup en ese repositorio. Se cerrará la operación con el siguiente mensaje: Ya se está ejecutando.

1. Introduzca el siguiente comando: programación de smo create -profile_name {[-full {-online | -offline | -auto}[-retain [-hora | -diario | -semanal | -mensual | -ilimitado] [-verify] | [-data [-filesfiles [ficheros]] | [-tablespaces [-destapaces [-unturnance]]-pathline | -untogpathline [-desteld.com]]]]-pathways] [-1]]-expointelgatment [-1]]]] [-pathways]]]-all-expointelgain] [-backup]] [-spanolet-all]] [-spanolet-all] [-ophora [-spanche]]]-spanche | -untilSCNuntilSCN | -until-dateyyyy-MM-dd HH:mm:ss | -before {-meses | -weeks | -days | -hours} -prune-destprune_dest1,prune_dest2] -schedule-namescommenteddd HH [-schedule-cronttime_comment] -<yyyy-MM-dd HH:mm> time-tasthand-time-time_time | -start | -time-time-time-time -time-time-time-time-time-time-time-start | -start | -time-time-time-time-time-start | -time-time-time-time-time -time-time-time-time-time-time-time-time-time-time-

Si desea…	Realice lo siguiente…
Programar una copia de seguridad de una base de datos en línea o sin conexión	Especifique -offline o -online para programar un backup de la base de datos sin conexión o en línea. Si especifica las opciones, no se puede utilizar -auto.
Deje que SnapManager gestione la programación de una base de datos independientemente de si está en línea o sin conexión	Especifique -auto. Si especifica -auto, no puede utilizar --offline o -online.
Programar una copia de seguridad de archivos de datos	Especifique -data -files para enumerar los archivos separados por comas. Por ejemplo, utilice los nombres de archivo f1,f2,f3.
Programar una copia de seguridad parcial de tablespaces específicos	Especifique -tablespaces para enumerar los tablespaces separados por comas. Por ejemplo, utilice ts1,ts2,ts3.

Programar copia de seguridad de archivos de registro de archivo	Especifique lo siguiente: • -archivelogs para programar la copia de seguridad de los archivos de registro de archivo • -backup-dest para programar los destinos de archivos de registro de archivos que se incluirán en el backup • -exclude-dest para programar los destinos de registro de archivos que se excluirán del backup
Especifique los valores de la clase de retención	Especifique -retain e indique si el backup debe conservarse de acuerdo con una de las siguientes clases de retención: • -cada hora • - diariamente • -semanal • -mensual • -El valor predeterminado de SnapManager ilimitado es cada hora.
Programar la eliminación de archivos de registro de archivos	Especifique lo siguiente: **-Prunelogs para afinar los archivos de registro de archivos mientras se programa una copia de seguridad** -prune-dest para especificar el destino de registro de archivos desde el que se recortan los archivos de registro de archivos
Incluya un nombre para el horario	Especifique -schedule-nombre.
Programar copia de seguridad de la base de datos en un intervalo de tiempo específico	Especifique la opción INTERVAL y seleccione el intervalo de tiempo entre las siguientes, mediante el cual deben crearse los backups: • -cada hora • - diariamente • -semanal • -mensual • -untimeonly

Configurar un horario	Especifique -cronstring e incluya las siguientes siete subexpresiones que describen la opción individual: • 1 se refiere a segundos. • 2 se refiere a minutos. • 3 se refiere a horas. • 4 se refiere a un día en un mes. • 5 se refiere al mes. • 6 se refiere a un día en una semana. • (Opcional) 7 se refiere al año. **Nota:** Si programó su copia de seguridad con diferentes horas en -cronstring y -start-time, entonces la programación de la copia de seguridad se sobrescribe y se activa por la -start-time.
Agregar un comentario sobre el programa de copia de seguridad	Specify -schedule-comment seguido de la cadena de descripción.
Especifique la hora de inicio de la operación de programación	Especifique -start-time en el formato yyyy-mm-dd hh:mm.
Cambiar el usuario de la operación de copia de seguridad programada mientras se programa la copia de seguridad	Especifique -runasuser. La operación se ejecuta como el usuario (usuario raíz o usuario de Oracle) que creó la programación. Sin embargo, puede utilizar su propio ID de usuario si tiene credenciales válidas tanto para el perfil de base de datos como para el host.
Active una actividad de tareas previas o posteriores a la tarea de la operación de programación de copia de seguridad mediante el archivo XML de especificación de tareas previas y posteriores	Especifique la opción -taskspec y proporcione la ruta absoluta del archivo XML de la especificación de la tarea para realizar un preprocesamiento o una actividad de post-procesamiento que tenga lugar antes o después de la operación de programación de copia de seguridad.

Actualizar una programación de backup

Puede ver una lista de operaciones programadas y actualizarlas si es necesario. Puede actualizar la frecuencia de programación, la hora de inicio de la programación, la expresión cronstring y el usuario que programó la copia de seguridad.

1. Para actualizar la programación de una copia de seguridad, introduzca este comando: smo schedule update -profile profile_name-schedule-namesetename [-schedule-commentschedule comment] -interval {-time | -Daily | -Weekly | -mensual | -onetimeonly} -start-timarttime-cronstringstring -runasrunususerosusuario [-quiet | -verbose]

Ver una lista de operaciones programadas

Es posible ver una lista de las operaciones programadas para un perfil.

1. Para mostrar información sobre operaciones programadas, introduzca este comando: smo schedule list -profile_name[-quiet | -verbose]

Suspensión de programaciones de backup

SnapManager permite suspender una programación de backup hasta que se reanude la programación de backup.

Puede suspender las programaciones activas. Si intenta suspender la programación de backup que ya se encuentra suspendida, es posible que aparezca el mensaje de error "no se puede suspender: Schedule <schedulename> ya en estado de suspensión".

1. Para suspender temporalmente la programación de la copia de seguridad, introduzca este comando: smo schedule suspend -profile_name-schedule-namesetnameName [-quiet | -verbose]

Reanudar programaciones de backup

Los administradores tienen la opción de reanudar la programación de backup suspendida.

Si intenta reanudar las programaciones activas, es posible que aparezca el mensaje de error "no se puede reanudar: Schedule <schedulename> ya en estado de reanudación".

1. Para reanudar la programación de backup suspendida, introduzca este comando: smo schedule resume -profile profile_name-schedule-namesetnamesetName [-quiet | -verbose]

Eliminación de programaciones de backup

Es posible eliminar programaciones de backup cuando ya no sean necesarias.

1. Para eliminar la programación de copia de seguridad, introduzca este comando: smo schedule delete -profile_name-schedule-namesetnameName [-quiet | -verbose]

Restaurar backups de base de datos

SnapManager para Oracle le permite restaurar una base de datos al estado que tenía cuando se tomó una copia Snapshot. Debido a que los backups se crean con más frecuencia, se reduce el número de registros que se debe aplicar, lo que reduce el tiempo medio de recuperación (MTTR) de una base de datos.

A continuación, se muestran algunas de las tareas que se pueden realizar en relación con la restauración y la recuperación de datos en bases de datos:

- Realice una restauración basada en archivos.
- Restaure todo el backup o parte del mismo.

  Cuando se restaura una parte de la misma, se especifica un grupo de espacios de tablas o un grupo de

archivos de datos. También puede restaurar los archivos de control junto con los datos o solo los propios archivos de control.

- Recupere los datos en función de un momento específico o de todos los registros disponibles, que almacena la última transacción comprometida con la base de datos.

  El punto en el tiempo puede ser un número de cambio de sistema (SCN) de Oracle o una fecha y hora (aaaa-mm-dd:hh:mm:ss). SnapManager utiliza el reloj de 24 horas.

- Restauración desde backups en el almacenamiento principal (backups locales).
- Restaurar y recuperar la copia de seguridad mediante SnapManager, o usar SnapManager para restaurar la copia de seguridad y utilizar otra herramienta, como Recovery Manager (RMAN), para recuperar los datos.
- Restaurar backups desde ubicaciones alternativas.

Para obtener más información, consulte *SnapManager for Oracle Best Practices*.

Puede restaurar una copia de seguridad realizada por una versión anterior de SnapManager utilizando SnapManager 3.0 y versiones posteriores.

Los administradores pueden realizar operaciones de restauración o recuperación mediante la interfaz gráfica de usuario (GUI) de SnapManager o mediante la interfaz de línea de comandos (CLI).

Información relacionada

Realizar backups de bases de datos

El comando smo backup restore

"Prácticas recomendadas de SnapManager para Oracle: media.netapp.com/documents/tr-3761.pdf"

Qué es la restauración de base de datos

SnapManager permite ejecutar operaciones de backup y restauración basadas en archivos.

En la siguiente tabla se describen los métodos de restauración:

Proceso de restauración	Detalles
Restauraciones basadas en archivos	Restauración de sistema de archivos completo en el almacenamiento (desde el principal o el secundario): SnapManager realiza una restauración completa del número de unidad lógica (LUN).

Restauración de todo el sistema de archivos en el lado del almacenamiento

Se realiza una restauración de sistema de archivos completo en el lado del almacenamiento cuando no es posible realizar una restauración de volumen, pero es posible restaurar todo el sistema de archivos en el sistema de almacenamiento.

Cuando se realiza una restauración del sistema de archivos en el almacenamiento, se produce lo siguiente:

- En un entorno SAN, todas las LUN utilizadas por el sistema de archivos (y el grupo de volúmenes subyacente, si las hubiera) se restauran en el sistema de almacenamiento.

Cuando se realiza una restauración del sistema de archivos en el almacenamiento, se produce lo siguiente, según la ubicación del almacenamiento:

- Cuando las restauraciones de SnapManager desde sistemas de almacenamiento primario, las LUN (SAN) se restauran in situ mediante SFSR.
- Cuando SnapManager restaura de los sistemas de almacenamiento secundario, las LUN (SAN) se copian desde los sistemas de almacenamiento secundario al sistema de almacenamiento principal a través de la red.

Como el sistema de archivos se restaura por completo, se revierten los archivos que no sean parte del backup. Se requiere una anulación si los archivos, que no forman parte de la restauración, se encuentran en el sistema de archivos que se está restaurando.

Restauración de archivos del lado del host

Una restauración de copias DE archivos del lado del host se usa como último recurso en entornos SAN cuando no se puede realizar la restauración del sistema de archivos del lado del almacenamiento ni la restauración de archivos del lado del almacenamiento.

Una restauración de copias de archivos del host implica las siguientes tareas:

- Clonar el almacenamiento
- Conectar el almacenamiento clonado al host
- Copiar archivos de los sistemas de archivos clonados de nuevo en los sistemas de archivos activos
- Desconectar el almacenamiento de clones del host
- Eliminar el almacenamiento del clon

Recuperación de backups

En SnapManager, se deben ejecutar las operaciones de restauración y recuperación al mismo tiempo. No se puede realizar una operación de restauración y, posteriormente, se puede realizar una operación de recuperación de SnapManager.

En SnapManager 3.2 o anterior, se puede utilizar SnapManager para restaurar y recuperar la copia de seguridad o utilizar SnapManager para restaurar la copia de seguridad y utilizar otra herramienta, como Oracle Recovery Manager (RMAN), para recuperar los datos. Puesto que SnapManager puede registrar sus copias de seguridad con RMAN, puede utilizar RMAN para restaurar y recuperar la base de datos con granularidades más finas como los bloques. Esta integración combina las ventajas de la velocidad y la eficiencia del espacio de las copias Snapshot con el nivel de control preciso para la restauración mediante RMAN.

> Debe recuperar una base de datos antes de poder utilizarla. Puede utilizar cualquier herramienta o script para recuperar una base de datos.

A partir de SnapManager 3.2 para Oracle, SnapManager permite restaurar automáticamente backups de bases de datos con los backups de registros de archivos. Incluso cuando los backups de registros de archivos están disponibles en la ubicación externa, SnapManager utiliza los backups de registros de archivos desde la ubicación externa para restaurar los backups de la base de datos.

Si se agregan nuevos archivos de datos a la base de datos, Oracle recomienda realizar una nueva copia de seguridad inmediatamente. Además, si restaura una copia de seguridad realizada antes de agregar los nuevos archivos de datos e intenta recuperar a un punto después de agregar los nuevos archivos de datos, el proceso de recuperación automática de Oracle podría fallar, ya que no puede crear archivos de datos. Consulte la documentación de Oracle para conocer el proceso de recuperación de los archivos de datos agregados después de una copia de seguridad.

Estado de la base de datos necesario para el proceso de restauración

El estado de la base de datos que se va a restaurar depende del tipo de proceso de restauración que se desee realizar y del tipo de archivos que se incluirán.

En la siguiente tabla, se muestra el estado en el que la base de datos debe estar según la opción de restauración seleccionada y el tipo de archivos que se desea incluir en la restauración:

Tipo de restauración	Archivos incluidos	Estado de la base de datos para esta instancia
Solo restauración	Archivos de control	Apagado
Archivos del sistema	Montaje o apagado	No hay archivos del sistema
Cualquier estado	Restauración y recuperación	Archivos de control
Apagado	Archivos del sistema	Montaje

El estado de la base de datos que requiere SnapManager para una operación de restauración depende del tipo de restauración que se ejecute (archivos completos, parciales o de control). SnapManager no realiza la transición de la base de datos a un estado inferior (por ejemplo, de Open a Mount) a menos que se especifique la opción force.

Qué planes de vista previa de restauración son

SnapManager ofrece planes de restauración antes y después de que se completa una operación de restauración. Los planes de restauración se utilizan para obtener una vista previa, revisar y analizar con respecto a los diferentes métodos de restauración.

Estructura del plan de restauración

El plan de restauración consta de las dos secciones siguientes:

- Vista previa/revisión: Esta sección describe cómo restaurará SnapManager cada archivo (o lo ha restaurado).
- Análisis: En esta sección se describe por qué no se utilizaron algunos mecanismos de restauración durante la operación de restauración.

La sección Vista previa/revisión

Esta sección muestra cómo se restaurará o se restaurará cada archivo. Al ver el plan de restauración antes de una operación de restauración, se denomina vista previa. Cuando se visualiza después de completar una operación de restauración, se denomina revisión.

El siguiente ejemplo de vista previa muestra que los archivos se restauran mediante los métodos de restauración del sistema de archivos del almacenamiento y restauración del sistema del almacenamiento. Para determinar por qué no se restaurarían todos los archivos utilizando el mismo método de restauración, consulte la sección Análisis.

```
Preview:
The following files will be restored completely via: storage side full
file system restore
E:\rac6\sysaux.dbf
E:\rac6\system.dbf
```

Cada método de restauración tiene una subsección que contiene información sobre los archivos que se pueden restaurar mediante ese método de restauración. Las subsecciones se ordenan según niveles decrecientes de eficiencia de los métodos de almacenamiento.

Es posible restaurar un archivo mediante varios métodos de restauración. Se utilizan varios métodos de restauración cuando los números de unidad lógica (LUN) subyacentes utilizados en un sistema de archivos se distribuyen entre los volúmenes del sistema de almacenamiento diferentes y algunos volúmenes son aptos para la restauración de volúmenes, mientras que otros no lo son. Si se utilizan varios métodos de restauración para restaurar el mismo archivo, la sección de vista previa será similar a la siguiente:

```
The following files will be restored via a combination of:
[storage side file system restore and storage side system restore]
```

La sección Análisis

La sección Análisis presenta las razones por las que algunos mecanismos de restauración no se utilizarán o no. Puede usar esta información para determinar qué es necesario para habilitar mecanismos de restauración más eficientes.

En el siguiente ejemplo se muestra una sección de análisis:

```
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.
```

En el ejemplo, puede anular el primer fallo desde la interfaz de línea de comandos (CLI) o seleccionando **Override** en la interfaz gráfica de usuario (GUI). El segundo fallo en las LUN asignadas del volumen es obligatorio y no se puede superar.

Puede resolver las comprobaciones haciendo lo siguiente:

- Para resolver un fallo de comprobación obligatorio, cambie el entorno de modo que se apruebe la comprobación.
- Para resolver un fallo de comprobación anulable, puede cambiar el entorno o anular la comprobación.

  Sin embargo, debe tener cuidado porque la anulación de la comprobación puede resultar en consecuencias no deseadas.

Previsualizar la información de restauración de copias de seguridad

Puede obtener una vista previa de la información sobre un proceso de restauración de backup antes de que se produzca para ver información sobre la idoneidad para la restauración que SnapManager para Oracle encontró en el backup. SnapManager analiza los datos del backup para determinar si el proceso de restauración puede completarse correctamente.

La vista previa de la restauración proporciona la siguiente información:

- Qué mecanismo de restauración (restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copia de archivos del lado del host) puede utilizarse para restaurar cada archivo.
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo al especificar la opción -verbose.

Si especifica la opción de vista previa en el comando backup restore, SnapManager no restaura nada, sino que enumera los archivos que se van a restaurar e indica cómo se restaurarán.

> Puede obtener una vista previa de todos los tipos de mecanismos de restauración. La vista previa muestra información acerca de un máximo de 20 archivos.

1. Introduzca el siguiente comando:smo backup restore -profileprofile_name-labellabel-complete -preview -verbose

   Por ejemplo, introduzca:

   ```
   smo backup restore -profile targetdb1_prof1
         -label full_bkup_sales_nov_08  -complete -preview -verbose
   ```

   En el siguiente ejemplo, se muestran los archivos listos para su restauración y se enumeran los diferentes métodos utilizados para cada uno:

   ```
   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. Revise los motivos por los que no pueden usarse otros procesos de restauración.
3. Inicie la operación de restauración sin la opción -preview, si sólo se muestran motivos que se pueden abreviar.

   Aún puede anular comprobaciones no obligatorias.

Restaurar backups en el almacenamiento principal

Es posible utilizar el comando backup restore para restaurar un backup de base de datos en el almacenamiento primario.

Es posible usar las opciones del comando backup restore para especificar si SnapManager debe restaurar todo el backup o parte de él. SnapManager también permite restaurar archivos de control junto con los archivos de datos o los espacios de tablas desde los backups en una sola operación de usuario. Se pueden incluir -controlfiles con -complete para restaurar archivos de control, junto con espacios de tablas y archivos de datos.

Se pueden seleccionar una de las siguientes opciones para restaurar el backup:

Si desea restaurar…	Usar…
Todo el backup con todos los espacios de tablas y ficheros de datos	-completo
Lista de tablespaces específicos	-tablespaces
Archivos de datos específicos	-archivos
Solo los archivos de control	-controlfiles
Espacios de tabla, archivos de datos y archivos de control	-complete -controlfiles

También puede restaurar el backup desde una ubicación alternativa especificando -restoreespec.

Si incluye -recover, puede recuperar la base de datos en:

- La última transacción que se produjo en la base de datos (todos los registros)
- Una fecha y hora específicas
- Un número de cambio de sistema (SCN) específico
- La hora del backup (sin registros)
- Solo restauración

> Tanto la recuperación de fecha y hora como la recuperación de SCN son recuperaciones puntuales.

SnapManager (3.2 o posterior) permite recuperar los backups de la base de datos restaurada automáticamente mediante los archivos de registro de archivos. Aunque los archivos de registro de archivos estén disponibles en la ubicación externa, si se especifica la opción -recover-from-location, SnapManager utiliza los archivos de registro de archivos de la ubicación externa para recuperar los backups de la base de datos restaurada.

Cuando se especifican las ubicaciones de los registros de archivo externos para la recuperación de los backups restaurados, debe asegurarse de incluir los nombres de la ubicación externa en mayúsculas. En el sistema de archivos, todos los nombres de carpetas y subcarpetas deben estar en mayúsculas, ya que Oracle convierte la ruta de destino en mayúscula y espera que las rutas de destino externas, los nombres de carpetas y los nombres de subcarpetas estén en mayúsculas. Si se especifican las rutas de destino de registros de archivo externos en minúscula, es posible que Oracle no pueda identificar la ruta especificada y no pueda restaurar la base de datos.

SnapManager proporciona la ubicación externa a Oracle. Sin embargo, Oracle no identifica los archivos desde el destino externo. Este comportamiento se aprecia en el destino de área de recuperación de flash. Se trata de problemas con Oracle y la solución alternativa es tener siempre una copia de seguridad de los archivos de registro de archivos en dichos diseños de bases de datos.

Si se proporciona un SCN o fecha incoherentes, la recuperación se detendrá en el último punto consistente recuperado con el mensaje de error recuperación correcta, pero insuficiente. Es necesario realizar manualmente la recuperación a un estado consistente.

Para la recuperación cuando no se aplican registros, SnapManager se recupera hasta el último SCN del último archivo de registro de archivos creado durante el backup. Si la base de datos es coherente hasta este SCN, la base de datos se abrirá correctamente. Si la base de datos no es coherente en este momento, SnapManager sigue intentando abrir la base de datos, que se abrirá correctamente si la base de datos ya es coherente.

SnapManager no admite la recuperación de los backups de solo registro de archivos.

Si el destino de los registros de archivos no es un almacenamiento compatible con Snapshot, SnapManager permite recuperar los backups de la base de datos restaurada mediante el perfil. Antes de ejecutar operaciones de SnapManager en un almacenamiento que no es compatible con Snapshot, debe añadir los destinos para archivedLogs.Exclude en smo.config.

Debe asegurarse de establecer el parámetro Exclude antes de crear un perfil. Sólo después de establecer el parámetro exclude en el archivo de configuración de SnapManager, la creación de perfiles se realiza correctamente.

Si el backup ya está montado, SnapManager no monta el backup de nuevo y utiliza el backup ya montado. Si la copia de seguridad está montada por un usuario diferente y si el usuario actual no tiene acceso a la copia de seguridad previamente montada, otros usuarios tienen que proporcionar los permisos. Todos los archivos de registro de archivos tienen permisos de lectura para los propietarios de los grupos; es posible que el usuario actual no obtenga los permisos, si el backup está montado por otro grupo de usuarios. Los usuarios pueden proporcionar permisos a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la restauración o recuperación.

Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de restauración correcta o con errores.

1. Introduzca el siguiente comando: smo backup restore -profile profile_name-label label-complete-recover -alllogs [-recover-from-locationpath [,path2]]-dump-verbose

   smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 - complete -recover -alllogs -verbose

2. Para restaurar datos en diferentes situaciones, complete una de las siguientes acciones:

Si desea restaurar…	Ejemplo de comando
Complete Database sin archivos de control y recupere un número SCN en particular (3794392). En este caso, existen los archivos de control actuales, pero todos los archivos de datos están dañados o perdidos. Restaure y recupere la base de datos de una copia de seguridad en línea completa existente a un punto inmediatamente anterior a ese SCN.	smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -until 3794392 -verbose
Completar la base de datos sin archivos de control y recuperar hasta una fecha y hora.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -until 2008-09-15:15:29:23 -verbose

Si desea restaurar…	Ejemplo de comando
Completar la base de datos sin archivos de control y recuperar hasta datos y tiempo. En este caso, existen los archivos de control actuales, pero todos los archivos de datos están dañados o se pierden o se produjo un error lógico después de un momento específico. Restaure y recupere la base de datos de una copia de seguridad en línea completa existente a una fecha y hora inmediatamente antes del punto de fallo.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -recover -until "2008-09-15:15:29:23" -verbose
Base de datos parcial (uno o más archivos de datos) sin archivos de control y recuperación mediante todos los registros disponibles. En este caso, existen los archivos de control actuales, pero uno o más archivos de datos están dañados o perdidos. Restaure esos archivos de datos y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	SMO backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -files E:\disks\s02.dbf E:\disks\salo03.dbf E:\disks\ventes04.dbf -recover -alllogs -verbose
Base de datos parcial (uno o más tablespaces) sin archivos de control y recuperación mediante todos los registros disponibles. En este caso, existen los archivos de control actuales, pero se pierden uno o más tablespaces o se pierde uno de los más archivos de datos pertenecientes al tablespace. Restaure esos tablespaces y recupere la base de datos a partir de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -tablespaces users -recover -alllogs -verbose
Sólo archivos de control y recuperación mediante todos los registros disponibles. En este caso, los archivos de datos existen, pero todos los archivos de control están dañados o perdidos. Restaure sólo los archivos de control y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	backup de smo restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -controlfiles -recover -alllogs -verbose

Si desea restaurar…	Ejemplo de comando
Complete la base de datos sin archivos de control y recupérese usando los archivos de control de copia de seguridad y todos los registros disponibles. En este caso, todos los archivos de datos están dañados o perdidos. Restaure sólo los archivos de control y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.	smo backup restore -profile targetdb1_pros1 -label full_bkup_sales_nov_08 -complete -using-backup -controulfile -recover -alllogs -verbose
Recupere la base de datos restaurada utilizando los archivos archive log de la ubicación externa del archive log.	smo backup restore -profile targetdb1_pros1 -label Full_bkup_sales_nov_08 -complete -using-backup -controulfile -recover -alllogs -recover-from-location E:\archive -verbose

3. Especifique las ubicaciones de los registros de archivos externos con la opción -recover-from-location.

Información relacionada

Restaurar backups desde una ubicación alternativa

El comando smo backup restore

Realizar recuperaciones a nivel de bloque con Oracle Recovery Manager (RMAN)

Puede configurar SnapManager para catalogar sus backups en Recovery Manager (RMAN), una herramienta de Oracle, de modo que pueda realizar una recuperación a nivel de bloque con RMAN. RMAN puede utilizar los archivos de control de la base de datos o una base de datos de catálogo de recuperación independiente como repositorio.

1. Para realizar un backup completo sin conexión mediante SnapManager, introduzca el siguiente comando:

   el backup de smo crea -offline-full-profeprofile_name-labelbackup_label_name-verbose

   Donde:

   - profile_name es el nombre del perfil asociado a la copia de seguridad
   - backup_label_name es el nombre de la etiqueta de backup

```
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. Para verificar que el backup está catalogado con RMAN, en el host de la base de datos, introduzca el siguiente comando en el símbolo del sistema de RMAN:

   listar etiqueta de datafilocopia tag_name;

2. Para verificar la base de datos y determinar si algún bloque está dañado, introduzca el siguiente comando:

   dbv FILE=user01.dbf

   La siguiente salida muestra que dos páginas están dañadas:

```
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. Para que los archivos de la copia de seguridad sean accesibles en el host y en RMAN, monte la copia de seguridad con el siguiente comando:

   montaje de backup de smo -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. Para recuperar los bloques, en RMAN, introduzca el siguiente comando:

   Blockrecover file "E:\path\file.dbf" 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. Para verificar si los bloques se han reparado, utilice el siguiente comando:

   dbv FILE=filename.dbf

   La siguiente salida muestra que ninguna página está dañada:

```
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)
```

   Todos los bloques dañados fueron reparados y restaurados.

Restaurar los archivos de una ubicación alternativa

SnapManager le permite restaurar archivos de datos y archivos de control desde una ubicación distinta a la de las copias Snapshot del volumen original.

La ubicación original es la ubicación del archivo en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es la ubicación desde la cual se restaurará un archivo.

Es posible restaurar desde una ubicación alternativa para restaurar los archivos de datos desde un sistema de archivos intermedio a un sistema de archivos activo.

SnapManager automatiza la recuperación. Al recuperar archivos de ubicaciones externas, SnapManager utiliza el comando recovery automatic from location.

SnapManager también usa Oracle Recovery Manager (RMAN) para recuperar archivos. Oracle debe reconocer los archivos que se van a recuperar. Los nombres de archivo deben tener el formato predeterminado. Al recuperarse del área de recuperación de flash, SnapManager ofrece la ruta traducida a Oracle. Sin embargo, Oracle no se recupera del área de recuperación de flash porque no puede generar el nombre de archivo correcto. Lo ideal es que el área de recuperación de flash sea un destino diseñado para trabajar con RMAN.

Información relacionada

Restaurar backups desde una ubicación alternativa

Para restaurar una copia de seguridad de la base de datos desde una ubicación alternativa, utilice los siguientes pasos principales, cada uno de los cuales se describe más adelante en esta sección.

- Realice una de las siguientes acciones, según la distribución de la base de datos y qué debe restaurarse:
  - Restaurar los archivos de datos necesarios desde cinta, SnapVault, SnapMirror o cualquier otro medio en cualquier sistema de archivos montado en el host de la base de datos.
  - Restaurar el sistema de archivos requerido y montarlo en el host de la base de datos.
  - Conéctese a los dispositivos RAW necesarios que existen en el host local.
- Cree un archivo XML (Lenguaje de marcado extensible) de especificación de restauración que incluya las asignaciones que SnapManager necesita para restaurar desde la ubicación alternativa a la ubicación original. Guarde el archivo en una ubicación a la que SnapManager pueda acceder.
- Utilice SnapManager para restaurar y recuperar los datos con el archivo XML de especificación de restauración.

Restauración de los datos de los archivos

Antes de restaurar desde una ubicación alternativa, debe restaurar los archivos necesarios desde cualquier medio de almacenamiento y restaurar los archivos de aplicaciones como SnapVault o SnapMirror a un sistema de archivos montado en el host local.

Es posible utilizar la restauración desde una operación de ubicación alternativa para copiar los archivos de un sistema de archivos alternativo a un sistema de archivos activo.

Debe especificar las ubicaciones alternativas desde las que desea restaurar los archivos originales mediante la creación de una especificación de restauración.

Restauración de datos desde el sistema de ficheros

Antes de restaurar datos desde una ubicación alternativa, debe restaurar el sistema de archivos necesario y montarlo en el host local.

Se puede invocar la operación de restauración desde una ubicación alternativa para copiar los archivos de sistemas de archivos alternativos a sistemas de archivos activos.

Para realizar esta operación, debe especificar los puntos de montaje alternativos desde los que se restaurarán los puntos de montaje originales y los nombres de las copias Snapshot originales creando un archivo de especificación de restauración.

> El nombre de copia Snapshot es un componente necesario porque el mismo sistema de archivos puede ajustarse varias veces en una única operación de backup (por ejemplo, una vez para los archivos de datos y otra para el archivo de registro).

Información relacionada

Creando especificaciones de restauración

El archivo de especificación de restauración es un archivo XML que contiene las ubicaciones originales y alternativas desde las que se puede restaurar el archivo. SnapManager utiliza este archivo de especificación para restaurar los archivos desde la ubicación especificada.

Puede crear el archivo de especificación de restauración usando cualquier editor de texto. Se debe usar la extensión .xml del archivo.

1. Abra un archivo de texto.
2. Introduzca lo siguiente: <restore-specification xmlns="" class="bare">http://www.netapp.com">
3. Introduzca cualquier información de asignación de archivos con el formato que se muestra en el ejemplo siguiente:

   ```
   <file-mapping>
       <original-location>E:\disks\sysaux.dbf</original-location>
       <alternate-location>E:\disks\sysaux.dbf</alternate-location>
   </file-mapping>
   ```

   La asignación de archivos especifica desde dónde se restaura un archivo. La ubicación original es la ubicación del archivo en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es la ubicación desde la que se restaura el archivo.

4. Introduzca cualquier información de asignación del sistema de archivos montado con el formato que se muestra en el ejemplo:

   ```
   <mountpoint-mapping>
        <original-location>E:\disks\sysaux.dbf</original-location>
        <snapname>snapname</snapname>
        <alternate-location>E:\disks\sysaux.dbf</alternate-location>
   </mountpoint-mapping>
   ```

   Mountpoint hace referencia a la ruta C:\myfs del directorio. La asignación de punto de montaje especifica el punto de montaje desde el que se restauran los archivos. La ubicación original es la ubicación del punto de montaje en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es el punto de montaje desde el que se restauran los archivos de la ubicación original. Snapname es el nombre de la copia Snapshot en la que se realizó el backup de los archivos originales.

   > El nombre de copia Snapshot es un componente necesario porque el mismo sistema de archivos se puede usar varias veces en una única operación de backup (por ejemplo, una vez para los archivos de datos y una vez para los registros).

5. Introduzca lo siguiente: </restore-specification>

6. Guarde el archivo como un archivo .xml y cierre la especificación.

Restaurar backups desde una ubicación alternativa

Es posible restaurar desde una ubicación alternativa para restaurar los archivos de datos desde un sistema de archivos intermedio a un sistema de archivos activo.

- Cree un archivo XML de especificación de restauración y especifique el tipo de método de restauración que desea utilizar.

Es posible usar el comando smo backup restore y especificar el archivo XML de especificación de restauración que se creó para restaurar el backup desde una ubicación alternativa.

1. Escriba el siguiente comando: smo backup restore -profileprofile-labellabel-complete-alllogs -restorespecirestoreespec

Información relacionada

El comando smo backup restore

Clonar el backup de bases de datos

Si clona una base de datos, puede realizar tareas como probar una actualización a una base de datos sin afectar a la base de datos en producción, duplicar una instalación maestra a varios sistemas de entrenamiento o duplicar una instalación maestra como instalación básica a otros servidores, que tienen requisitos similares.

Puede ejecutar las siguientes tareas relacionadas con la clonado:

- Clonar una base de datos a partir de un backup existente.
- Clonar una base de datos en su estado actual, lo que permite crear el backup y el clon en un procedimiento.
- Clone una base de datos y utilice scripts de plugins personalizados, que se ejecutan antes o después de la operación de clonado.
- Clone una base de datos en el mismo host en el que reside la base de datos.
- Clone una base de datos con los archivos de registro de archivos desde la ubicación del registro de archivos externo.
- Clonar una base de datos en un host alternativo.
- Consulte una lista de clones.
- Ver información detallada sobre clones.
- Eliminar clones.

Qué es la clonación

Puede clonar una base de datos para crear una réplica exacta de la base de datos original. Es posible crear el clon a partir de un backup completo o desde el estado actual de la base de datos.

A continuación se presentan algunas de las ventajas de crear un clon con SnapManager:

Ventajas	Detalles
Velocidad	La operación de clonación de SnapManager usa la función FlexClone disponible con Data ONTAP. Esto permite clonar rápidamente grandes volúmenes de datos.
Gestión eficiente del espacio	Cuando crea un clon con SnapManager, solo se necesita espacio para los cambios entre el backup y el clon. Un clon SnapManager es una copia Snapshot editable de la base de datos original y puede crecer según sea necesario. Por el contrario, un clon físico de la base de datos requiere que disponga de espacio suficiente para copiar la base de datos completa.
Copia virtual	Puede utilizar la base de datos clonada como si fuera la base de datos original. Por ejemplo, puede usar un clon para pruebas, comprobaciones de plataformas y actualizaciones, simulaciones múltiples aplicadas a un conjunto de datos de gran tamaño, y pruebas y almacenamiento provisional en oficinas remotas. Los cambios en el clon no afectan a la base de datos original. Una vez clonada la base, la base de datos clonada queda totalmente operativa.
Sencillez	Es posible clonar una base de datos a cualquier host con los comandos de SnapManager.

Para poder clonar una base de datos, debe asegurarse de que se cumplen los siguientes requisitos previos:

- Elimine el archivo speLing <SID>.ora de $ORACLE_HOME\database.
- Elimine el archivo OLET <SID>.ora de $ORACLE_HOME\database.
- Elimine los destinos de volcado de Oracle que estén especificados en el archivo de especificación del clon.
- Elimine los archivos de control de Oracle que estén especificados en el archivo de especificación del clon.
- Elimine los archivos de registro de recuperación de Oracle especificados en el archivo de especificación del clon.

Debe proporcionar al clon un nuevo identificador del sistema. No se pueden ejecutar simultáneamente dos bases de datos con el mismo identificador de sistema en el mismo host. Es posible tener un clon en otro host con el mismo identificador de sistema. Es posible asignar al clon una etiqueta o dejar que SnapManager cree una etiqueta con el identificador del sistema, la fecha y la hora en que se creó el clon.

Cuando introduce una etiqueta, no debe incluir espacios ni caracteres especiales.

Como parte del proceso de clonado, SnapManager crea los parámetros y archivos de Oracle necesarios para la base de datos clonada. Un ejemplo de un archivo de Oracle necesario es el archivo <SID>.ora de Re.

Cuando se clona una base de datos, SnapManager crea un nuevo archivo <SID>.ora para la base de datos en el directorio $ORACLE_HOME\database.

Cuando SnapManager clona el almacenamiento de una base de datos, también crea un nuevo punto de montaje del sistema de archivos, pero no cambia la estructura de directorio en el punto de montaje desde la CLI de SnapManager. No obstante, desde la interfaz gráfica de usuario de SnapManager, es posible cambiar la estructura de directorio y los metadatos del sistema de archivos.

Es posible clonar un backup de base de datos en el host en el que reside la base de datos o en un host alternativo.

Si la base de datos clonada utilizaba un archivo spfile, SnapManager crea un archivo spfile para el clon. Coloca este archivo en el directorio $ORACLE_HOME\database y crea la estructura de directorio para los archivos de diagnóstico. el nombre de archivo es spfile <SID>.ora.

Métodos de clonación

Es posible clonar una base de datos mediante uno de estos dos métodos. El método seleccionado afecta a la operación de creación de clon.

En la siguiente tabla se describen los métodos de clonado y su efecto en la operación clone create y su opción -reserve. Una LUN se puede clonar mediante cualquiera de los dos métodos.

Método de clonación
Descripción
clone create -reserve
Clonado de LUN
Se crea un nuevo LUN clon en el mismo volumen.
Cuando -reserve para una LUN está establecida en yes, se reserva espacio para todo el tamaño de LUN dentro del volumen.
Clonado de volúmenes
Se crea un nuevo FlexClone y la LUN clonada existe dentro del nuevo volumen clonado. Utiliza la tecnología FlexClone.
Cuando -reserve para un volumen está establecida en yes, se reserva espacio para todo el tamaño del volumen dentro del agregado.

Creando especificaciones de clon

SnapManager para Oracle utiliza un archivo XML de especificación del clon, que incluye las asignaciones, las opciones y los parámetros que se deben utilizar en la operación de clonado. SnapManager utiliza esta información para determinar dónde colocar los archivos que clona y cómo tratar información de diagnóstico, archivos de control, parámetros, etc.

Es posible crear el archivo de especificación del clon con la interfaz gráfica de usuario (GUI) de SnapManager, la interfaz de línea de comandos (CLI) o un editor de texto.

Cuando crea el archivo de especificación del clon con un editor de texto, debe guardarlo como archivo .xml. Es posible usar este archivo XML para otras operaciones de clonado.

También puede crear una plantilla de especificación de clon y personalizarla. Puede usar el comando de plantilla de clon de smo o la interfaz gráfica de usuario; use el asistente Clone.

SnapManager para Oracle agrega una cadena de versión a cualquier plantilla de especificación de clon que genere. SnapManager para Oracle asume la versión más reciente de cualquier archivo de especificación del clon que no tenga una cadena de versión.

Si desea realizar la clonado remota, no cambie las ubicaciones predeterminadas de los archivos de datos, los archivos de registro de recuperación y los archivos de control en el archivo de especificación del clon. Si cambia la ubicación predeterminada, SnapManager no puede crear el clon o crear el clon en una base de datos que no es compatible con la funcionalidad de Snapshot. Por lo tanto, la creación automática de perfil falla.

> Aunque la información del punto de montaje y del grupo de discos de ASM se puede editar desde la interfaz gráfica de usuario, solo se puede cambiar el nombre del archivo y no las ubicaciones del archivo.

Puede ejecutar una tarea varias veces, ya sea con combinaciones de parámetros y valores iguales o diferentes.

1. Abra un archivo de texto e introduzca texto como se muestra en el ejemplo siguiente:

```
<clone-specification xmlns="http://www.example.com>
     <storage-specification/>
     <database-specification/>
 </clone-specification>
```

2. En el componente de especificación de almacenamiento, introduzca los puntos de montaje para los archivos de datos.

   La especificación de almacenamiento enumera las ubicaciones para el nuevo almacenamiento creado para el clon, como puntos de montaje de archivos de datos y dispositivos sin formato. Estos elementos se deben asignar del origen al destino.

   En el ejemplo siguiente se muestra la sintaxis de punto de montaje del archivo de datos que se utiliza en la especificación del clon:

```
<mountpoint>
     <source>\mnt\path\source_data file_mountpoint</source>
     <destination>\mnt\path\target_data file_mountpoint</destination>
</mountpoint>
```

3. En el componente de especificación de la base de datos, identifique la información del archivo de control como una lista de los archivos de control que desea crear para el clon.

La especificación de la base de datos especifica las opciones de la base de datos para el clon, como los archivos de control, los registros de recuperación, los registros de archivos y los parámetros de Oracle.

En el ejemplo siguiente se muestra la sintaxis del archivo de control que se utiliza en la especificación del clon:

```
<controlfiles>
     <file>\mnt\path\clonename\control\control01.ctl</file>
     <file>\mnt\path\clonename\control\control02.ctl</file>
</controlfiles>
```

4. Especifique la estructura del registro de recuperación para el clon.

   En el ejemplo siguiente se muestra la estructura de directorio redo log para la clonado:

```
<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. Especifique los parámetros de Oracle que deben establecerse con diferentes valores en la base de datos clonada. Si utiliza Oracle 10, debe especificar los siguientes parámetros:
   - Volcado en segundo plano
   - Volcado de memoria
   - Volcado de usuario
   - (Opcional) registros de archivo

   > Si los valores de los parámetros no están configurados correctamente, la operación de clonado se detiene y se recibe un mensaje de error.

   Si no especifica la ubicación donde se almacenan los registros de archivos, SnapManager crea el clon en modo noarchivelog. SnapManager copia esta información de parámetro en el archivo init.ora del clon.

   + en el ejemplo siguiente se muestra la sintaxis de parámetros que se utiliza en la especificación del clon:

```
<parameters>
     <parameter>
          <name>log_archive_dest_1</name>
          <value>LOCATION=\mnt\path\clonename\archive</value>
     </parameter>
</parameters>
```

+ + puede utilizar un valor predeterminado utilizando un elemento default dentro del elemento Parameter. En el ejemplo siguiente, el parámetro os_Authentication_PREFIX tomará el valor predeterminado porque se especifica el elemento predeterminado:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <default></default>
     </parameter>
</parameters>
```

+ + puede especificar una cadena vacía como valor de un parámetro mediante un elemento vacío. En el ejemplo siguiente, os_Authentication_PREFIX se establecerá en una cadena vacía:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <value></value>
     </parameter>
</parameters>
```

+ + NOTA: Puede utilizar el valor del archivo init.ora de la base de datos de origen para el parámetro sin especificar ningún elemento.

+ + Si un parámetro tiene varios valores, puede proporcionar los valores de los parámetros separados por comas. Por ejemplo, si desea mover los archivos de datos de una ubicación a otra, puede utilizar el parámetro dB_file_name_convert y especificar las rutas de acceso del archivo de datos separadas por comas, como se muestra en el ejemplo siguiente:

+

+

+

```
<parameters>
     <parameter>
          <name>db_file_name_convert</name>
          <value>>\mnt\path\clonename\data file1,\mnt\path\clonename\data
file2</value>
     </parameter>
</parameters>
```

+ + Si desea mover los archivos de registro de una ubicación a otra, puede utilizar el parámetro log_file_name_convert y especificar las rutas de acceso del archivo de registro separadas por comas, como se muestra en el siguiente ejemplo:

+

+

+

```
<parameters>
     <parameter>
          <name>log_file_name_convert</name>

<value>>\mnt\path\clonename\archivle1,\mnt\path\clonename\archivle2</value
>
     </parameter>
</parameters>
```

1. Opcional: Especifique sentencias SQL arbitrarias para que se ejecuten en el clon cuando está en línea.

   Puede utilizar las sentencias SQL para realizar tareas como la recreación de los archivos temporales en la base de datos clonada.

   > Debe asegurarse de que no se incluya un punto y coma al final de la instrucción SQL.

   A continuación se muestra una sentencia SQL de muestra que se ejecuta como parte de la operación de clonado:

```
<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>
```

Ejemplo de especificación del clon

En el ejemplo siguiente se muestra la estructura de especificaciones de clon, incluidos los componentes de especificación de base de datos y almacenamiento, para un entorno de Windows:

```
<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>
```

Información relacionada

Clonar bases de datos y usar scripts de plugins personalizados

Clonar bases de datos a partir de backups

Clonado de bases de datos en estado actual

Consideraciones para clonar una base de datos en un host alternativo

Clonar bases de datos y usar scripts de plugins personalizados

SnapManager proporciona un método para usar scripts personalizados antes y después de que se produzca una operación de clonado. Por ejemplo, podría haber creado un script personalizado que valida un SID de base de datos de clon y garantiza que el SID lo permita la política de nomenclatura. Mediante el plugin de clonado de SnapManager, puede incluir scripts personalizados y hacerlos ejecutar automáticamente antes o después de una operación de clonado de SnapManager.

1. Ver scripts de plugins de muestra.
2. Cree una secuencia de comandos desde cero o modifique una de las secuencias de comandos del plug-in de ejemplo.

   Cree su script personalizado de acuerdo con las directrices de script del plugin de SnapManager.

3. Coloque la secuencia de comandos personalizada en una ubicación de directorio especificada.
4. Actualice el archivo XML de especificación del clon e incluya información sobre el script personalizado que debe utilizarse durante el proceso de clonado.
5. Mediante un comando de SnapManager, compruebe que los scripts personalizados estén operativos.
6. Cuando inicia la operación de clonado, incluya el nombre de script y los parámetros opcionales.

Clonar bases de datos a partir de backups

Es posible clonar una base de datos a partir de un backup con el comando clone create.

Primero debe crear un archivo de especificación del clon para la base de datos. SnapManager crea el clon según la información de este archivo de especificación.

Debe proporcionar al clon un nuevo identificador del sistema de Oracle (SID). No se pueden ejecutar dos bases de datos con el mismo SID simultáneamente en el mismo host. Puede tener un clon en otro host que utiliza el mismo SID. Para designar un nombre único para el clon, utilice -label. Si no utiliza esta opción, SnapManager crea un nombre único para el clon que incluye el SID, fecha y hora.

Después de clonar una base de datos, es posible que desee actualizar los archivos tnsnames.ora en los equipos cliente con la nueva información de conexión de base de datos clonada. Los archivos tnsnames.ora se utilizan para conectarse a una instancia de Oracle sin tener que especificar la información completa de la base de datos. SnapManager no actualiza los archivos tnsnames.ora.

SnapManager siempre crea un backup, incluidos los archivos de registro de archivos, si se utiliza el perfil creado con backups -include-con-en-línea. SnapManager permite clonar únicamente los backups completos de la base de datos.

SnapManager (3.2 o posterior) permite clonar los backups que contienen los archivos de datos y los archivos de registro de archivos.

Si el registro de archivos está disponible desde una ubicación externa, puede especificar la ubicación externa durante la clonado para recuperar la base de datos clonada en un estado coherente. Debe asegurarse de que Oracle pueda acceder a la ubicación externa. No se admite la clonado de backups de solo registro de archivos.

Aunque se crea el backup de registros de archivos junto con el backup parcial en línea, no se puede crear un clon de la base de datos con este backup.

Cuando se especifican las ubicaciones de los registros de archivos externos para recuperar la base de datos clonada en un estado coherente, debe asegurarse de incluir los nombres de las ubicaciones externas completamente en mayúsculas. En el sistema de archivos, los nombres de todas las carpetas y subcarpetas deben estar en mayúscula porque la base de datos Oracle convierte la ruta de destino en mayúscula y espera que las rutas de destino externas, los nombres de carpetas y los nombres de subcarpetas estén en mayúsculas. Si se especifican las rutas de destino de registros de archivo externos en minúscula, es posible que la base de datos no pueda identificar la ruta especificada y no se pueda recuperar la base de datos clonada.

Es posible clonar el backup de base de datos desde la ubicación de archivo de registro de archivos externo solo para una base de datos independiente.

Puede especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de creación de clones con errores o correctamente.

Clonación de copia de seguridad de archivo de datos sin copia de seguridad de archivo de registro

Cuando el backup de archivos de datos no incluye el backup de registros de archivo, SnapManager para Oracle clona la base de datos según el número de cambio del sistema (SCN) registrado durante el backup. Si no se puede recuperar la base de datos clonada, se muestra el mensaje de error archivo de registro archivado de <number> de subproceso y <SCN> de cambio necesario para completar la recuperación, a pesar de que SnapManager para Oracle sigue clonando la base de datos y, finalmente, se realiza correctamente la creación del clon.

Al clonar con el backup de archivos de datos sin incluir el backup de registros de archivos, SnapManager recupera la base de datos clonada hasta el último SCN de registro de archivos, que se registra durante el backup.

1. Cree un archivo de especificación del clon.
2. Para crear un clon, introduzca el siguiente comando: smo clone create -backup-labelbackup_name -newsidnew_sid-labelclone_label-profileprofile_name-clonespecpath_to_clonespecfile [-taskspectaskspec] [-recover-from-location] path1 [,<path2>…][-dump]]

Información relacionada

Clonado de bases de datos en estado actual

Consideraciones para clonar una base de datos en un host alternativo

Creando especificaciones de clon

El comando smo clone create

Crear scripts de tareas previas, tareas posteriores y directivas

Variables disponibles en los scripts de tareas para la operación de clonado

Creación de scripts de tareas

Almacenamiento de los scripts de tareas

Clonado de bases de datos en estado actual

Puede crear un backup y un clon de la base de datos desde el estado actual de la base

de datos mediante un solo comando.

Cuando especifica el perfil con la opción -current, SnapManager crea primero un backup y, a continuación, un clon del estado actual de la base de datos.

En la configuración de perfil, si habilitó el backup de archivos de datos y registros de archivos juntos para la clonado, siempre que se realice un backup de los archivos de datos en línea, también se realizará un backup de los registros de archivos. Al clonar la base de datos, SnapManager crea el backup de archivos de datos junto con el backup del registro de archivos y crea el clon de la base de datos. Si no se incluye el backup de registros de archivos, SnapManager no crea el backup de registros de archivos y, por lo tanto, no puede crear el clon de la base de datos.

1. Para clonar la base de datos en su estado actual, introduzca el siguiente comando: smo clone create -profileprofile_name-current -labelclone_name-clonespecclonespec.xml

   Este comando realiza un backup completo automático (generando la etiqueta de backup) e inmediatamente crea un clon a partir de ese backup mediante una especificación de clon existente que desea utilizar.

   > Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de las operaciones realizadas correctamente o con errores. El volcado se recoge tanto para las operaciones de backup como de clonado.

Clonado de backups de bases de datos sin necesidad de restablecer registros

SnapManager le permite realizar clonados flexibles, de modo que puede recuperar la base de datos clonada manualmente en un momento determinado sin necesidad de abrir la base de datos mediante reaslogs. También puede configurar manualmente la base de datos clonada como una base de datos en espera de Data Guard.

Cuando se puede seleccionar la opción -no-resetlogs mientras se crea el clon, SnapManager realiza las siguientes actividades para crear la base de datos clonada:

1. Ejecuta la actividad de tarea de preprocesamiento, si se especifica, antes de iniciar la operación de clonado
2. Crea la base de datos clonada con el SID especificado por el usuario
3. Ejecuta las sentencias SQL emitidas con la base de datos clonada.

   Sólo se ejecutan correctamente las sentencias SQL que se pueden ejecutar en estado de montaje.

4. Ejecuta la actividad de la tarea de posprocesamiento, si se especifica.

Qué tareas debe realizar para recuperar la base de datos clonada manualmente

1. Monte los backups de registros de archivos y recupere la base de datos clonada manualmente mediante los archivos de registro de archivos desde la ruta montada.
2. Después de realizar la recuperación manual, abra la opción recovery cloned database with -reaslogs.
3. Cree espacios de tablas temporales, si es necesario.
4. Ejecute la utilidad DBNEWID.
5. Conceda un privilegio sysdba a las credenciales de la base de datos clonada.

Mientras se clonan los backups de la base de datos mediante la opción -no-resetlogs, SnapManager deja la base de datos clonada en el estado montado para poder realizar una recuperación manual.

> La base de datos clonada creada con la opción -no-resetlogs no es una base de datos completa. Por lo tanto, no debe ejecutar ninguna operación de SnapManager en esta base de datos, si bien SnapManager no le restringe la posibilidad de realizar ninguna operación.

Si no se especifica la opción -no-resetlogs, SnapManager aplica los archivos de registro de archivos y abre la base de datos con resetlogs.

1. Introduzca el siguiente comando: smo clone create -profileprofile_name [-backup-labelbackup_name | -backup-idbackup_id | current] -newsidnew_sid-clonespecfull_path_to_clonespecfile-no-resetlogs

   Si intenta especificar las opciones -no-resetlogs y Recover-from-location, SnapManager no le permite especificar ambas opciones juntas y muestra el mensaje de error: SMO-04084: Debe especificar una de las opciones: -No-resetlogs o -recover-from-location.

Ejemplo

```
smo clone create -profile product -backup-label full_offline -newsid
PROD_CLONE -clonespec prod_clonespec.xml -label prod_clone-reserve -no
-reset-logs
```

Consideraciones para clonar una base de datos en un host alternativo

Para poder clonar en un host distinto al que reside la base de datos, deben cumplirse algunos requisitos.

En la siguiente tabla se muestran los requisitos de configuración del host de origen y de destino:

Requisitos previos de configuración	Requisito
Arquitectura	Debe ser igual en los hosts de origen y objetivo
Sistema operativo y versión	Debe ser igual en los hosts de origen y objetivo
SnapManager para Oracle	Se debe instalar y ejecutar en los hosts de origen y objetivo
Credenciales	Se debe configurar para que el usuario acceda al host de destino
Oracle	Se debe instalar la misma versión de software en los hosts de origen y destino. Oracle Listener debe ejecutarse en el host de destino.
Pila de almacenamiento compatible	Debe ser igual en los hosts de origen y objetivo

Protocolo utilizado para acceder a los archivos de datos	Debe ser igual en los hosts de origen y objetivo
Dominio	Tanto el host remoto como el host en el que reside la base de datos deben estar en el dominio y no en el grupo de trabajo

Clonar una base de datos en un host alternativo

Puede utilizar el comando clone create para clonar un backup de base de datos en un host alternativo.

- Cree un perfil o tenga un perfil existente.
- Crear una copia de seguridad completa o tener una copia de seguridad de la base de datos existente.
- Cree una especificación de clon o tenga una especificación de clon existente.
  a. Para clonar una base de datos en un host alternativo, introduzca el siguiente comando: smo clone create -backup-label backup_label_name-newsid new_sid-host target_host-label clone_label-commentcomment_text-profileprofile_name-clonefilespec full_path_to_clonesfile

     Oracle no permite ejecutar dos bases de datos con el mismo SID simultáneamente en el mismo host. Por este motivo, debe suministrar un SID nuevo para cada clon. Sin embargo, puede tener una base de datos en otro host con el mismo SID.

Información relacionada

Creación de perfiles

Clonar bases de datos a partir de backups

Creando especificaciones de clon

El comando smo clone create

Ver una lista de clones

Puede ver una lista de clones asociados con un perfil determinado.

La lista incluye la siguiente información sobre los clones de un perfil:

- El ID del clon
- Estado de la operación de clonado
- SID de Oracle para el clon
- Host donde reside el clon
- Etiqueta del clon

Si especifica la opción -verbose, la salida también muestra los comentarios introducidos para el clon.

1. Para mostrar una lista de todos los clones de un perfil, introduzca el siguiente comando smo clone list -profile_name [-quiet | -verbose]

Información relacionada

El comando smo clone list

Visualización de información detallada de los clones

Puede ver información detallada sobre un clon específico mediante el comando clone show.

El comando clone show muestra la siguiente información:

- Identificador del sistema del clon e ID del clon
- Estado de la operación de clonado
- Clonar crear fecha y hora de inicio y finalización
- Etiqueta del clon
- Clonar comentario
- Etiqueta e ID de copia de seguridad
- Base de datos de origen
- Hora de inicio y de finalización de la copia de seguridad
- Nombre de la base de datos, tablespaces y archivos de datos
- El nombre del host y los sistemas de archivos que contienen archivos de datos
- Los volúmenes del sistema de almacenamiento y las copias Snapshot respaldan el clon
  a. Introduzca el siguiente comando: smo clone show -profile profile_name [-label label | -id guid]

Información relacionada

El comando smo clone show

Eliminar clones

Puede eliminar los clones cuando el tamaño de la copia Snapshot alcance entre un 10% y un 20% del backup. Así también se garantiza que el clon tenga los datos más recientes.

La etiqueta es el identificador único de cada clon en un perfil. Puede usar la etiqueta o el ID del clon, pero no el identificador del sistema (SID) para eliminar el clon.

El SID del clon y la etiqueta del clon no son iguales.

Cuando elimina un clon, la base de datos debe estar en ejecución. De lo contrario, no se eliminarán muchos ficheros y directorios del clon existente, lo que hará que se realice más trabajo antes de crear otro clon.

Los directorios especificados para ciertos parámetros de Oracle del clon se destruyen cuando se elimina el clon y solo deben contener datos para la base de datos clonada: Destinos de registro de archivo, destinos de fondo, núcleo y destinos de volcado de usuario. No se eliminan los archivos de auditoría.

No es posible eliminar un clon cuando se utiliza en otras operaciones.

Opcionalmente, es posible recoger los archivos de volcado después de una operación de eliminación de clonado correcta o con errores.

1. Introduzca el siguiente comando: smo clone delete -profile profile_name [-label label label label | -id guid] [-force][-dump][-quiet]|[-verbose]

Ejemplo

```
smo clone delete -profile targetdb1_prof1 -label sales0908_clone1
```

Información relacionada

El comando smo clone delete

Introducción a la protección de datos en SnapManager

SnapManager admite protección de datos para proteger los backups en sistemas de almacenamiento secundarios o terciarios. Debe configurar las relaciones de SnapMirror y SnapVault entre los volúmenes de origen y de destino.

Puede utilizar las secuencias de comandos posteriores al backup tanto desde la interfaz de línea de comandos (CLI) como desde la interfaz gráfica de usuario (GUI) para proteger los backups en un sistema de almacenamiento principal.

Cómo SnapManager retiene los backups en el almacenamiento local

SnapManager permite crear backups que cumplen las políticas de retención, lo cual especifica cuántos backups se deben conservar correctamente en el almacenamiento local. Puede especificar la cantidad de backups correctos que debe conservarse en el perfil de una determinada base de datos.

Es posible crear backups para lo siguiente:

- 10 días de backup diarios en almacenamiento primario
- 2 meses de backups mensuales en almacenamiento primario
- 7 días de backup diarios en almacenamiento secundario
- 4 semanas de backups semanales en el almacenamiento secundario
- 6 meses de backups mensuales en almacenamiento secundario

Para cada perfil de SnapManager, puede cambiar los valores de las siguientes clases de retención no limitadas:

- Cada hora
- Todos los días
- Semanal
- Mensual

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Un backup caduca cuando su antigüedad supera el período de retención establecido para su clase de retención o la cantidad de backups supera el número de retenciones. Por ejemplo, si el número de backup es 15 (SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups elegibles más antiguos caducan.

Cuando se caduca un backup, SnapManager libera o elimina el backup caducado. SnapManager siempre conserva el último backup realizado.

SnapManager solo cuenta la cantidad de backups realizados correctamente para el número de retención y no considera lo siguiente:

Backups no incluidos en el número de retención	Detalles adicionales
Backups con errores	SnapManager conserva la información sobre backups realizados correctamente y sin errores. Aunque los backups sin éxito requieren solo un espacio mínimo en el repositorio, es posible que desee eliminarlos. Los backups sin éxito permanecen en el repositorio hasta que se eliminan.
Backups designados para retenerse en cuenta de forma ilimitada o con backups para otra clase de retención	SnapManager no elimina los backups designados para que se conserven de forma ilimitada. Además, SnapManager solo considera los backups en la misma clase de retención (por ejemplo, SnapManager sólo considera los backups por horas para el número de retención por horas).
Backups montados desde el almacenamiento local	Cuando se montan las copias Snapshot, también se clonan y por lo que no se consideran aptos para la retención. SnapManager no puede eliminar las copias Snapshot si están clonadas.
Backups que se utilizan para crear un clon en el almacenamiento local	SnapManager conserva todos los backups que se usan para crear clones, pero no los considera para el número de retención de backups.

SnapManager proporciona un recuento de retención y una duración predeterminados para cada clase de retención. Por ejemplo, para el recuento de clases de retención cada hora, SnapManager, de forma predeterminada, retiene cuatro backups por hora. Puede anular estos valores predeterminados y establecer los valores al crear o actualizar el perfil, o cambiar los valores predeterminados para el recuento de retenciones y la duración en el archivo smo.config.

Cuando los backups locales caducan según su política de retención, los backups se eliminan.

En una operación de backup solo de archivado, SnapManager no archiva los archivos de registro de recuperación, a diferencia del proceso de backup de base de datos en línea. Debe agregar una secuencia de comandos de pretarea para archivar los archivos redo log antes de realizar la operación de copia de seguridad de archivvelog-only. La secuencia de comandos de pretarea debe ejecutar el comando ALTER System switch logfile.

El siguiente ejemplo muestra las acciones que SnapManager realiza en diversos tipos de backups, según una

política de retención de backups de tres días (con el número establecido en retener 3):

Fecha de la copia de seguridad	Estado	Se han adoptado medidas para la política de retención	Explicación
5/10	Exitoso	Mantenga	Este es el backup exitoso más reciente, por lo que se mantendrá.
5/9	Clonado correcto	Omitir	SnapManager no considera los backups utilizados para la clonado en el número de políticas de retención. Este backup se omite del número de backups realizados correctamente.
5/8	Correcto, montado	Omitir	SnapManager no considera los backups montados en el número de políticas de retención. Este backup se omite del número de backups realizados correctamente.
5/7	Error	Omitir	Los backups con errores no se cuentan.
5/5	Exitoso	Mantenga	SnapManager mantiene este segundo backup diario de éxito.
5/3	Exitoso	Mantenga	SnapManager mantiene este tercer backup diario de éxito.
5/2	Exitoso	Eliminar	SnapManager cuenta este backup correctamente, pero después de que SnapManager alcanza tres backups diarios correctos, este backup se elimina.

Información relacionada

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Aspectos que se deben tener en cuenta al realizar la protección de datos

Debe tener en cuenta ciertas consideraciones para realizar la protección de datos.

- Para realizar operaciones de clonado o restauración desde sistemas secundarios, se debe montar el volumen de destino en el espacio de nombres y exportarlo correctamente.
- Para deshabilitar el parámetro SnapDrive Configuration, compruebe-export-permision-nfs-clone, debe establecer el valor como off.

  La documentación de SnapDrive para UNIX en el sitio de soporte de NetApp contiene información adicional sobre el parámetro check-export-permision-nfs-clone.

- Debe configurar la relación de SnapMirror para los volúmenes de almacenamiento secundario solicitados en el sistema de almacenamiento secundario.
- Debe configurar la relación de SnapVault para los qtrees de almacenamiento secundario solicitados en el sistema de almacenamiento secundario para Data ONTAP que funciona en 7-Mode.
- Debe definir una política y reglas para la etiqueta de SnapMirror definida por el usuario si utiliza SnapVault post-script para Clustered Data ONTAP.

  La copia posterior de SnapVault es compatible con los volúmenes de Clustered Data ONTAP y los tipos de relación de SnapMirror DP y XDP. La documentación de ONTAP en el sitio de soporte de NetApp contiene información sobre la configuración de SnapMirror y SnapVault.

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Licencias necesarias para la protección de datos en SnapManager

Debe asegurarse de que las licencias requeridas para la protección de datos estén instaladas y habilitadas en los sistemas de almacenamiento primario y secundario.

Los sistemas de almacenamiento primario reciben las últimas actualizaciones de transacciones para la base de datos Oracle, almacenan los datos y proporcionan protección de copia de seguridad local de la base de datos. El sistema de almacenamiento principal también conserva los archivos de datos de la base de datos, los archivos de registro y los archivos de control. Los sistemas de almacenamiento secundario actúan como almacenamiento remoto para los backups protegidos.

Para la protección de datos, deben instalarse y activarse las siguientes licencias en los sistemas de almacenamiento primario:

> Si desea habilitar la protección de datos en los sistemas de almacenamiento secundario, también debe instalar y habilitar estas licencias en los sistemas de almacenamiento secundario.

- Data ONTAP funcionando en 7-Mode (7.3.1 o posterior) o en Clustered Data ONTAP (8.2 o posterior)
- SnapVault
- SnapRestore
- SnapMirror
- Se requiere FlexClone para el clonado.

  Además, FlexClone es necesario para la red de área de almacenamiento (SAN) solo si SnapDrive está configurado para utilizar FlexClone en entornos SAN.

- El protocolo adecuado, por ejemplo, Internet Small Computer System Interface (iSCSI) o Fibre Channel (FC).

Protección de backups de bases de datos mediante scripts posteriores

SnapManager permite proteger backups de bases de datos mediante scripts posteriores cuando se establece la relación de SnapMirror o SnapVault entre los sistemas de almacenamiento primario y secundario. Se pueden usar los scripts posteriores predeterminados para la actividad de procesamiento posterior de la operación de backup desde la interfaz de línea de comandos de SnapManager y la interfaz gráfica de usuario.

Es posible usar los siguientes scripts posteriores predeterminados disponibles en default_install_Directory\plugins\backup\create\post:

- snapmirror postscript, Mirror_the_backup.cmd si utiliza Data ONTAP en 7-Mode
- script posterior de SnapVault, Vault_the_backup.cmd si utiliza Data ONTAP en 7-Mode
- snapmirror postscript, Mirror_the_backup_CDOT.cmd si utiliza Clustered Data ONTAP
- script posterior de SnapVault, Vault_the_backup_CDOT.cmd si utiliza Clustered Data ONTAP

Para obtener más información, consulte el archivo readme.txt disponible en default_install_directory\plugins.

SnapManager 3.1 o versiones anteriores proporciona scripts de procesamiento previo o de posprocesamiento solo para operaciones de clonado. A partir de la versión 3.2 de SnapManager se proporcionan scripts de procesamiento previo y de posprocesamiento para operaciones de backup y restauración. Es posible usar estos scripts para ejecutarse antes o después de las operaciones de backup o restauración.

> Los scripts se proporcionan sólo como referencia. Se han probado con SnapDrive 7.0 para Windows o posterior, pero es posible que no funcionen en todos los entornos. Debe personalizar los scripts según sus requisitos de protección secundarios. Los scripts no funcionan con las versiones de SnapDrive anteriores a la 6.2.

Ejemplos de scripts posteriores

Puede consultar los scripts de ejemplo y crear scripts personalizados basados en su entorno para realizar mirroring y almacenamiento remoto. Los scripts de ejemplo están disponibles en default_install_directory\plugins\backup\create\post.

Mirror_the_backup.cmd

Si utiliza Data ONTAP en 7-Mode, es posible utilizar este script de muestra para reflejar el backup. Incluye tres operaciones (comprobación, descripción y ejecución) y las ejecuta al final del script. La secuencia de comandos también incluye el manejo de mensajes de error con códigos de 0 a 4 y > 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

Si utiliza Data ONTAP en 7-Mode, es posible utilizar este script de ejemplo para almacenar el backup. Incluye tres operaciones (comprobación, descripción y ejecución) y las ejecuta al final del script. La secuencia de comandos también incluye el manejo de mensajes de error con códigos de 0 a 4 y > 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

Si utiliza Clustered Data ONTAP, puede utilizar este script de ejemplo para reflejar el backup. Incluye tres operaciones (comprobación, descripción y ejecución) y las ejecuta al final del script. La secuencia de comandos también incluye el manejo de mensajes de error con códigos de 0 a 4 y > 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

Si utiliza Clustered Data ONTAP, puede utilizar este script de ejemplo para almacenar el backup. Incluye tres operaciones (comprobación, descripción y ejecución) y las ejecuta al final del script. La secuencia de comandos también incluye el manejo de mensajes de error con códigos de 0 a 4 y > 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%
```

Creación o actualización de los scripts posteriores

Puede crear nuevos scripts de post o utilizar los scripts disponibles en default_install_directory\plugins\backup\create\post.

Es necesario estructurar el script de una forma concreta para poder ejecutarlo dentro del contexto de una operación de SnapManager. Cree el script en función de las operaciones esperadas, los parámetros de entrada disponibles y las convenciones de código de retorno.

1. Cree un nuevo script o utilice los scripts de ejemplo disponibles.
2. Modifique o incluya las funciones, variables y parámetros según sea necesario.
3. Guarde el script personalizado.
4. Agregue el nombre del script y las entradas necesarias en el archivo XML de especificación de tareas de posprocesamiento o proporcione las entradas desde la GUI seleccionando el parámetro de entrada y script adecuado.

> No es necesario proporcionar detalles de almacenamiento secundario en el archivo XML de especificación de tareas.

Información relacionada

Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager

Creación de archivos de post-procesamiento y de especificación de tareas

SnapManager permite crear archivos XML de especificación de tareas de posprocesamiento para la operación de backup que incluyen los scripts posteriores de SnapMirror o SnapVault. Los scripts permiten reflejar o almacenar el backup en el almacenamiento secundario.

1. Abra un nuevo archivo XML.

   Puede ver el archivo XML de ejemplo de especificación de tareas disponible en default_install_directory\plugins\Examples.

2. Agregue el nombre del script como parámetro de entrada.
3. Guarde el archivo XML de especificación de tareas.

Uso de la especificación de tareas de posprocesamiento para reflejar volúmenes

SnapManager para Oracle permite usar el script para reflejar los volúmenes después de que se produce la operación de backup en un entorno Windows.

1. Cree un archivo XML de especificación de tarea.
2. En el archivo XML, introduzca el nombre del script como un parámetro de entrada.
3. Guarde el archivo XML de especificación de tareas.
4. Cree un backup protegido de la base de datos en el almacenamiento secundario con el siguiente comando.

   Al crear la copia de seguridad protegida, debe proporcionar la ruta de acceso completa del archivo XML de especificación de tareas guardado después de la opción -taskspec .

   Ejemplo: Smobackup create -profile test_profile -full -online -taskspec "C:\\mirror\\snapmirror.xml"

En el ejemplo siguiente se muestra una estructura de especificación de tareas de posprocesamiento si está utilizando Data ONTAP en 7-Mode:

```
#     <post-tasks>
#               <task>
#                   <name>Mirror the backup</name>
#                    <description>Mirror the backup</description>
#               </task>
#             <post-tasks>
```

El siguiente ejemplo muestra una estructura de especificación de tareas de posprocesamiento si utiliza Clustered Data ONTAP:

```
# <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>
```

Uso de la especificación de tareas de posprocesamiento para los qtrees de almacén

SnapManager para Oracle permite utilizar el script para almacenar los qtrees una vez que la operación de backup se lleva a cabo en un entorno de Windows.

1. Cree un archivo XML de especificación de tarea.
2. En el archivo XML, introduzca el nombre del script como un parámetro de entrada.
3. Guarde el archivo XML de especificación de tareas.
4. Cree un backup protegido de la base de datos en el almacenamiento secundario con el siguiente comando.

   Al crear la copia de seguridad protegida, debe proporcionar la ruta de acceso completa del archivo XML de especificación de tareas guardado después de la opción -taskspec .

   Ejemplo: Smobackup create -profile test_profile -full -online -taskspec "C:\\mirror\\snapvault.xml"

En el ejemplo siguiente se muestra la estructura de especificación de tareas de posprocesamiento si está utilizando Data ONTAP en 7-Mode:

```
# <post-tasks>
#                <task>
#                  <name>Vault the backup</name>
#                   <description>Vault the backup</description>
#              </task>
#         <post-tasks>
```

En el siguiente ejemplo se muestra la estructura de especificación de tareas de posprocesamiento si se utiliza Clustered Data ONTAP:

```
# <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>
```

Realizando operaciones de gestión

Es posible realizar tareas de gestión después de instalar y configurar SnapManager. Estas tareas le permiten gestionar las operaciones normales más allá del backup, la restauración y la clonación.

Los administradores pueden realizar operaciones mediante la interfaz gráfica de usuario o la interfaz de línea de comandos.

Ver una lista de operaciones

Es posible ver una lista con un resumen de todas las operaciones realizadas en un perfil.

Puede ver la siguiente información cuando enumere operaciones asociadas a un perfil en particular:

- Fecha de inicio y finalización cuando se ejecutó la operación
- Estado de la operación
- ID de la operación
- Tipo de operación
- Host en el que se ejecutó

  a. Para enumerar la información resumida de todas las operaciones, utilice el siguiente comando: smo operation list profile -profile profile_name-delimitador character [-quiet | -verbose]

     Cuando se especifica la opción -delimitador, el comando enumera cada fila en una línea separada y los atributos de esa fila están separados por el carácter especificado.

Información relacionada

El comando smo operation list

Ver los detalles de la operación

Puede ver información detallada acerca de un perfil determinado para verificar el éxito o

el fracaso de una operación. También puede ayudar a determinar los recursos de almacenamiento que se están utilizando para una operación en particular.

Es posible ver los siguientes detalles sobre una operación en particular:

- ID de la operación
- Tipo de operación
- Si la operación se ha forzado
- Información de tiempo de ejecución, incluido el estado, la fecha de inicio y de finalización de la operación
- El host donde se ejecutó la operación, incluidos el ID de proceso y la versión de SnapManager
- Información del repositorio
- Recursos de almacenamiento en uso
  a. Para ver la información detallada de un ID de operación específico, introduzca el siguiente comando: SMO operation show -profile profile_name [-label label | -id] [-quiet | -verbose]

Información relacionada

El comando smo operation show

Emitir comandos desde un host alternativo

Puede emitir comandos de la CLI desde un host distinto al host de la base de datos y SnapManager enrutará los comandos que introduzca al host adecuado.

Para que el sistema pueda enviar una operación al host correcto, primero debe saber dónde encontrar el perfil para la operación. En este procedimiento, el sistema mantiene el perfil en la información de asignación de repositorios para un archivo en el directorio principal del usuario en el host local.

1. Para que el directorio principal del usuario local sea consciente de las asignaciones de perfil a repositorio de modo que pueda enrutar la solicitud de operación, introduzca el siguiente comando: smo profile SYNC -repository-dbname repo_dbname-host repo_host-Port repo_Port-login-username repo_username [-quiet | -verbose]

Comprobación de la versión del software SnapManager

Puede determinar qué versión del producto se ejecuta en el host local ejecutando el comando version.

1. Para comprobar la versión de SnapManager, introduzca este comando: Versión de smo

Información relacionada

El comando version de smo

Detener el servidor host SnapManager

Cuando termine de utilizar SnapManager, quizás desee detener el servidor.

1. Para detener el servidor, escriba el siguiente comando, como usuario raíz: smo_Server stop

Información relacionada

El comando smo_Server stop

Reiniciar el servidor host SnapManager

Puede reiniciar el servidor SnapManager a través de la ventana Servicios.

1. Haga clic en **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. En la ventana Services, seleccione NetAppSnapManager 3.3 para Oracle.
3. Puede reiniciar el servidor de una de las siguientes maneras:
   a. En el panel izquierdo, haga clic en **Reiniciar**.
   b. Haga clic con el botón derecho en NetAppSnapManager 3.3 para Oracle y seleccione **Restart** en el menú desplegable.
   c. Haga doble clic en NetAppSnapManager 3.3 para Oracle y, en la ventana de propiedades que se abre, haga clic en **Reiniciar**.

Desinstalando SnapManager

Puede desinstalar SnapManager del servidor host.

- Detenga el servidor host antes de desinstalar SnapManager.
  a. Haga clic en **Inicio** > **Panel de control** > **Agregar o quitar programas**.
  b. Seleccione **SnapManager para Oracle**.
  c. Haga clic en **Desinstalar**.

Configuración de una notificación por correo electrónico

SnapManager permite recibir una notificación por correo electrónico acerca del estado de finalización de las operaciones de base de datos ejecutadas por perfil. SnapManager genera el correo electrónico y ayuda a realizar la acción adecuada en función del estado de finalización de la operación de la base de datos. La configuración de las notificaciones por correo electrónico es un parámetro opcional.

Puede configurar una notificación por correo electrónico para un perfil individual como notificación de perfil y para varios perfiles en una base de datos de repositorio como notificación de resumen.

Notificación de perfiles

Para un perfil individual, es posible recibir un correo electrónico para las operaciones de base de datos correctas o fallidas.

> De forma predeterminada, la notificación por correo electrónico está habilitada para las operaciones con bases de datos fallidas.

Notificación de resumen

La notificación de resumen permite recibir un mensaje de correo electrónico resumido sobre las operaciones

de la base de datos realizadas mediante varios perfiles. Se pueden habilitar notificaciones por hora, por día, por semana o por mes.

> En SnapManager 3.3, las notificaciones de resumen se envían solo si se especifica el servidor host que tiene que enviar la notificación. Si se actualiza SnapManager desde una versión anterior a 3.3, es posible que las notificaciones de resumen no se envíen si no se especificó el servidor host en la configuración de notificaciones de resumen.

> Si crea un repositorio en un nodo de una base de datos que se encuentra en un entorno RAC y habilita la notificación de resumen, posteriormente cuando agrega el mismo repositorio a otro nodo de la base de datos, el correo electrónico de notificación de resumen se envía dos veces.

Puede usar notificación a nivel de perfil o notificación de resumen al mismo tiempo.

SnapManager habilita la notificación por correo electrónico para las siguientes operaciones de bases de datos ejecutadas por perfiles:

- Crear backup en el almacenamiento principal
- Restaurar backups
- Crear clones
- Verificar backups

Después de crear o actualizar perfiles con la notificación de correo electrónico activada, puede desactivarla. Si deshabilita la notificación por correo electrónico, ya no recibirá alertas por correo electrónico para esas operaciones de base de datos ejecutadas por perfil.

El correo electrónico que recibe contiene los siguientes detalles:

- Nombre de la operación de base de datos, por ejemplo, backup, restauración o clonado
- Nombre de perfil utilizado para la operación de base de datos
- Nombre del servidor host
- Identificador del sistema de la base de datos
- Hora de inicio y finalización de la operación de base de datos
- Estado de la operación de base de datos
- Mensaje de error, si lo hay
- Mensajes de advertencia, si los hay

Puede configurar lo siguiente:

- Servidor de correo para un repositorio
- Notificación por correo electrónico de un nuevo perfil
- Notificación por correo electrónico de un perfil existente
- Notificación por correo electrónico de resumen para varios perfiles en un repositorio

> Es posible configurar las notificaciones por correo electrónico desde la interfaz de línea de comandos (CLI) y la interfaz gráfica de usuario (GUI).

Configuración de un servidor de correo para un repositorio

SnapManager permite especificar los detalles del servidor de correo desde los cuales se envían las alertas por correo electrónico.

SnapManager permite especificar el nombre de host o la dirección IP del servidor de correo electrónico del remitente y el número de puerto del servidor de correo electrónico para un nombre de la base de datos de repositorio que requiere la notificación por correo electrónico. Puede configurar el número de puerto del servidor de correo en un intervalo comprendido entre 0 y 65535; el valor predeterminado es 25. Si requiere autenticación para la dirección de correo electrónico, puede especificar el nombre de usuario y la contraseña.

Debe especificar el nombre o la dirección IP del servidor host que maneja la notificación por correo electrónico.

1. Para configurar el servidor de correo para que envíe alertas por correo electrónico, introduzca el siguiente comando: smo notification set -sender-emailemail_address-mailhosthost-mailportmailport [-authentication-usernameusername-passwordpassword] -repository_Port-dbnamerepo_service-hostrepo_host-login -usernamerepo_username

   Las demás opciones para este comando son las siguientes:

   [-fuerza]

Para hacer lo siguiente…	Realice lo siguiente…
Para especificar la dirección de correo electrónico del remitente.	Especifique la opción -sender-email. En SnapManager 3.2 para Oracle, puede incluir guión (-) al especificar el nombre de dominio de la dirección de correo electrónico. Por ejemplo, puede especificar la dirección de correo electrónico del remitente como -sender-emailuser@org-corp.com.
Para especificar el nombre de host o la dirección IP del servidor de correo electrónico del remitente.	Especifique la opción -mailhost.
Especificar el número de puerto del servidor de correo electrónico para un nombre de base de datos de repositorio que requiere notificación por correo electrónico. Puede configurar el número de puerto del servidor de correo en un intervalo comprendido entre cero y 65535; el valor predeterminado es 25.	Especifique la opción -mailport.
Especifique el nombre de usuario y la contraseña si necesita autenticación para la dirección de correo electrónico.	Especifique la opción -Authentication seguida del nombre de usuario y la contraseña.

En el siguiente ejemplo se configura el servidor de correo.

```
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
```

Configuración de la notificación por correo electrónico para un perfil nuevo

Cuando se crea un perfil nuevo, se puede configurar para recibir una notificación por correo electrónico al finalizar la operación de la base de datos.

- Debe configurar la dirección de correo electrónico desde la cual se envían las alertas.
- Debe usar una lista separada por comas para varias direcciones de correo electrónico.

  Debe asegurarse de que no hay espacio entre la coma y la siguiente dirección de correo electrónico.

  > Asegúrese de introducir el conjunto de direcciones de correo electrónico entre comillas dobles.

  a. Introduzca el siguiente comando: smo profile create -profileprofile [-profile-passwordprofile_password] -repository [-dbnamercompenso_service_name-hotpo_host-portrepo_Port-login-usernamerepo] [-nombre-nombre-usuario_base-dbnamedb] [-nombre_nombre_usuario]-nombredeusuario_archivo] [-nombredeusuario_archivo-did]-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredearchivo-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario]-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario] [-archivo

     Las demás opciones para este comando son las siguientes:

     [-fuerza]

     > SnapManager admite hasta 1000 caracteres para las direcciones de correo electrónico.

     Cuando se crea un backup de archivos de datos y archivos de registro de archivos junto con el perfil (para crear backups de registros de archivos independientes) y se produce un error en la creación del backup de archivos de datos, la notificación por correo electrónico se envía con el backup de datos como nombre de la operación en lugar de un backup de datos y un backup de registros de archivos. Cuando la operación de backup de archivo de datos y archivo de registro de archivo se realiza correctamente, se muestra el resultado de la siguiente manera:

```
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  :
```

Personalización del asunto del correo electrónico para un nuevo perfil

Puede personalizar el asunto del correo electrónico para el nuevo perfil cuando lo cree.

Puede personalizar el asunto del correo electrónico utilizando el patrón {profile}_{operation-name}_{dB-sid}_{dB-host}_{start-date}_{end-date}_{status} o bien introducir su propio texto.

Nombre de la variable	Descripción	Valor de ejemplo
perfil	Nombre de perfil utilizado para la operación de base de datos	PROF1
nombre-operación	Nombre de la operación de base de datos	Backup, copia de seguridad de datos, copia de seguridad de registros de datos y archivos
db-sid	SID de la base de datos	DB1
host de base de datos	Nombre del servidor host	Hosta
fecha de inicio	La hora de inicio de la operación de la base de datos en el formato mdd:hh:ss yyyy	Abril 27 21:00:45 PST 2012
fecha de finalización	Hora de finalización de la operación de la base de datos en el formato mdd:hh:ss yyyy	Abril 27 21:10:45 PST 2012
estado	Estado de la operación de base de datos	Correcto

Si no se proporciona ningún valor para las variables, SnapManager muestra el siguiente mensaje de error: Faltan valores -Subject.

1. Introduzca el siguiente comando: smo profile create -profileprofile [-profile-passwordprofile_password] -repository_service_name-hostrepo_portrepo_Port-login-usuarios1 [-nombredeusuario-base-dbnamedb_dbnombre_dbnombre_host] [-diserondname] [-diserondnemail-directnnombre_nombre_usuario]]-nombredeusuario-nombredeusuario] [-nombredeusuario-

nombredeusuario_archivo]-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario-nombredeusuario-nombredeusuario] [-nombredeusuario-nombredeusuario]-nombredeusuario-nombredeusuario] [-archivo

Configuración de la notificación por correo electrónico para un perfil existente

Al actualizar un perfil, puede configurar para recibir una notificación por correo electrónico al finalizar la operación de la base de datos.

- Debe configurar la dirección de correo electrónico desde la cual se envían las alertas.
- Debe introducir una sola dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas.

  Puede usar una lista separada por comas para varias direcciones. Debe asegurarse de que no hay espacio entre la coma y la siguiente dirección de correo electrónico. Si lo desea, también puede añadir un asunto al correo electrónico.

  > Debe asegurarse de introducir el conjunto de varias direcciones de correo electrónico entre comillas dobles.

  a. Introduzca el siguiente comando:actualización del perfil de smo -profileprofile [-profile-passwordprofile_password][-database-dbnamedb_dbname-host dB_host [-siddb_sid] [-login -usernamedb_username-password_password-Port_Port] [{-directnemail] [-diseronsb]-directnemail] [_subject]-directndtnb]] [-directntndtndtndtndtntndtndtnb]]] [-directnemail]]-directndtndtndtn] [-directnenc]-directn] [-directnemail]-subdtndtndtndtn]] [-directndtndtndtndtndtndtn] [-email]]] [-subdtndtndtndtndtndtndtn]] [-email]]

     La opción Success se puede utilizar para recibir una notificación únicamente sobre las operaciones de base de datos correctas y la opción Failure para recibir una notificación solo sobre las operaciones de base de datos fallidas.

Personalización del asunto del correo electrónico para un perfil existente

SnapManager le permite personalizar el patrón de asunto del correo electrónico para un perfil existente actualizando dicho perfil. Este patrón de asunto personalizado sólo es aplicable al perfil actualizado.

1. Introduzca el siguiente comando: smo profile update -profileprofile [-profile-passwordprofile_password][-database-dbnombrecompensb_dbname-host dB_host [-siddb_sid] [-login -usernamedb_username -password_password-Port_Port] [{-dirección-nombre-usuario] [-nombredeusuario_archivo_archivo]]-archivo_contraseña]-disoc] [-disoc]-disoc-nombredeusuario] [-archivo]-disoc-archivo]-nombredeusuario-archivo]-disoc-archivo]-disoc-disoc]-disoc-disoc] [-archivo]-disoc-disoc-archivo]-disoc-disoc-disoc-archivo]-disoc] [-disoc-disoc-disoc] [-disoc-disoc-disoc] [-disopnoarchivo]-disoc-disoc-disoc]-disoc-disoc-disoc] [-nombre

Configuración de notificación por correo electrónico de resumen para varios perfiles

SnapManager permite configurar una notificación por correo electrónico de resumen para varios perfiles en una base de datos de repositorio.

Es posible configurar el host del servidor SnapManager como host de notificación desde el cual se envía el correo electrónico de notificación de resumen a los destinatarios. Si se cambian el nombre de host o la dirección IP del servidor SnapManager, también se puede actualizar el host de notificación.

Puede seleccionar cualquiera de las horas de programación en las que se requiera una notificación por correo electrónico:

- Hourly: Para recibir una notificación por correo electrónico cada hora
- Diario: Para recibir una notificación por correo electrónico diariamente
- Semanal: Para recibir una notificación por correo electrónico semanalmente
- Mensual: Recibir una notificación por correo electrónico mensualmente

Debe introducir una sola dirección de correo electrónico o una lista de direcciones de correo electrónico separadas por comas para recibir notificaciones de las operaciones realizadas mediante dichos perfiles. Asegúrese de que no haya espacio entre la coma y la siguiente dirección de correo electrónico cuando introduzca varias direcciones de correo electrónico.

> Debe asegurarse de introducir el conjunto de varias direcciones de correo electrónico entre comillas dobles.

SnapManager le permite añadir un asunto de correo electrónico personalizado utilizando las siguientes variables:

- Nombre de perfil utilizado para la operación de base de datos.
- Nombre de la base de datos
- SID de la base de datos
- Nombre del servidor host
- Hora de inicio de la operación de la base de datos en el formato yyyymmdd:hh:ss
- Hora de finalización de la operación de la base de datos en el formato yyyymmdd:hh:ss
- Estado de la operación de base de datos

Si selecciona no agregar un asunto personalizado, SnapManager muestra un mensaje de error: Falta valor -asunto.

1. Introduzca el siguiente comando: Notificación de smo update-summary-notification -repository -portrepo_Port-dbnamerepo_service_name-hstrepo_host-login-usernamerepo_username -emailmail_dirección1,email_directs2-subjectSubject-patterm-frequency {-day-profiletime_time | -1|3 -time|4|31-time|1-time|5|6-time|7-time|1-time|1-time||1-time|1-time||-time|1-time|1-time|1-time|1||1-time|1 -time|1|-time|-time|1-time|

   Las demás opciones para este comando son las siguientes:

   [-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
```

Adición de un nuevo perfil para resumir las notificaciones por correo electrónico

Después de configurar una notificación por correo electrónico de resumen para la base de datos de repositorio, puede agregar un nuevo perfil a la notificación de resumen utilizando el comando summary notification.

1. Introduzca el siguiente comando: smo profile create -profileprofile_name [-profile-passwordprofile_password] -reposisero_service_name-hostrepo_host-portrepo_Port-login-usernamerepo [-nombre_base-dbedb_dbedb_nombre_nombre_host] [-nombre_nombre_usuario_base_datos_usuario]-nombre_archivo]-nombre_usuario_usuario_usuario] [-nombre_usuario_archivo-archivo]-nombre_archivo-nombre_contraseña]-nombre_archivo]-nombre_usuario-nombre_archivo-nombre_archivo-nombre_archivo-nombre_archivo]]-nombre_nombre_usuario-nombre_archivo-nombre_d] [-nombre_usuario-nombre_usuario-nombre_archivo]-nombre_usuario-nombre_usuario-nombre_usuario-nombre_usuario]]-nombre_d] [-nombre_usuario-nombre_nombre_archivo]-nombre_archivo-nombre_archivo-nombre_usuario-nombre_archivo]-nombredeusuario-nombre_usuario-nombre_archivo] [-nombre_archivo-nombre_archivo]-d_

   Las demás opciones para este comando son las siguientes:

   [-fuerza]

Adición de un perfil existente para resumir las notificaciones por correo electrónico

SnapManager le permite añadir un perfil existente a una notificación de correo electrónico de resumen al actualizar dicho perfil.

1. Introduzca el siguiente comando: smo profile update -profileprofile_name [-profile-passwordprofile_password] -reposisero_service_name-hostrepo_host-portrepo_Port-login -ususernamerepo [-nombre_base-dbedb_dbedb_nombre_nombre_hostDB]-nombre_host [-nombre_did_usuario_did]-did]-disermb]-nombre_usuariob]-nombre_nombre_nombre_nombre_usuariob] [-nombre_nombre_nombre_nombre_nombre_nombre_nombre_usuario]-nombre_nombre_nombre_usuario]-nombre_d]-nombre_usuariob]-nombre_usuariob]-nombre_usuariob]-nombre_nombre_nombre_nombre_nombre_d]-nombre_nombre_nombre_nombre_usuariob] [-usuariob] [-nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_nombre_usuario]-nombre_nombre_nombre_d]-nombre_nombre_d]-usuariob]-

Desactivar la notificación por correo electrónico para varios perfiles

Después de activar la notificación de resumen por correo electrónico para varios perfiles, puede desactivarlos para que ya no reciban alertas por correo electrónico.

SnapManager permite deshabilitar la notificación de resumen por correo electrónico para esas operaciones de la base de datos ejecutadas por perfil. En la interfaz de línea de comandos de SnapManager, introduzca el

comando notification remove-summary para deshabilitar la notificación por correo electrónico de resumen de varios perfiles, así como el nombre de la base de datos del repositorio para la cual no se requiere notificación por correo electrónico.

1. Para deshabilitar la notificación de resumen para varios perfiles en una base de datos de repositorio, escriba el siguiente comando: SMO notification remove-summary-notification -repository-portrepo_Port -dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username

En el siguiente ejemplo se muestra la desactivación de la notificación de resumen para varios perfiles en una base de datos de repositorio:

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5
```

Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager

SnapManager para Oracle utiliza un archivo XML (lenguaje de marcado extensible) de especificación de tareas que indica las tareas previas y las tareas posteriores para las operaciones de copia de seguridad, restauración y clonado. Es posible añadir los nombres de las tareas previas y las secuencias de comandos posteriores a las tareas en el archivo XML para que las tareas se realicen antes o después de las operaciones de backup, restauración y clonado.

En SnapManager (3.1 o anterior), puede ejecutar los scripts de tareas previas y posteriores a la tarea solo para la operación de clonado. En SnapManager (3.2 o posterior) para Oracle, puede ejecutar las secuencias de comandos previas y posteriores a la tarea para las operaciones de backup, restauración y clonado.

En SnapManager (3.1 o anterior), la sección de especificación de tareas forma parte del archivo XML de especificación del clon. Desde SnapManager 3.2 para Oracle, la sección de especificación de tareas es un archivo XML independiente.

> SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.

En SnapManager (3.2 o posterior) para Oracle, debe asegurarse de que se cumplan las siguientes condiciones para que las operaciones de SnapManager se realicen correctamente:

- Para las operaciones de copia de seguridad y restauración, utilice el archivo XML de especificación de tareas.
- Para la operación de clonado, proporcione dos archivos de especificación: Un archivo XML de especificación del clon y un archivo XML de especificación de tareas.

  Si desea habilitar la actividad de tareas previas o posteriores a la tarea, también puede agregar el archivo XML de especificación de tareas.

Puede crear el archivo de especificación de la tarea mediante la interfaz gráfica de usuario (GUI) de SnapManager, la interfaz de línea de comandos (CLI) o un editor de texto. Debe utilizar una extensión .xml

para el archivo con el fin de habilitar las características de edición adecuadas. Puede guardar este archivo para usarlo para operaciones de backup, restauración y clonado futuras.

El archivo XML de especificación de tareas incluye dos secciones:

- La sección de tareas previas incluye scripts que se pueden ejecutar antes de las operaciones de backup, restauración y clonado.
- La sección tareas posteriores incluye scripts que se pueden ejecutar después de las operaciones de backup, restauración y clonado.

Los valores incluidos en las secciones de tareas previas y tareas posteriores deben cumplir las siguientes directrices:

- Nombre de la tarea: El nombre de la tarea debe coincidir con el nombre del script, que se muestra cuando se ejecuta el comando plugin.sh -describe.

  > Si hay un error de coincidencia, es posible que reciba el siguiente mensaje de error: El archivo no encontrado.

- Nombre del parámetro: El nombre del parámetro debe ser una cadena que se puede utilizar como valor de variable de entorno.

  La cadena debe coincidir con el nombre del parámetro en el script personalizado, que se muestra cuando se ejecuta el comando plugin.sh -describe .

Puede crear el archivo de especificación según la estructura del siguiente archivo de especificación de tareas de ejemplo:

```
<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>
```

El archivo XML de especificación de tareas no debe contener ninguna directiva.

En la interfaz gráfica de usuario de SnapManager, es posible establecer el valor del parámetro y guardar el archivo XML. Puede utilizar la página activación de tareas del asistente Crear copia de seguridad, del asistente Restaurar o recuperación y del asistente Crear copia de seguridad, para cargar el archivo XML de especificación de tareas existente y utilizar el archivo seleccionado para la actividad de tareas previas o posteriores a la tarea.

Una tarea se puede ejecutar varias veces, ya sea con combinaciones de parámetros y valores iguales o diferentes. Por ejemplo, puede utilizar una tarea Guardar para guardar varios archivos.

SnapManager utiliza las etiquetas XML que se proporcionan en el archivo de especificación de tareas para el procesamiento previo o la actividad de posprocesamiento para las operaciones de backup, restauración y clonado, independientemente de la extensión del archivo de especificación de la tarea.

Crear scripts de tareas previas, tareas posteriores y directivas

SnapManager le permite crear los scripts para la actividad de procesamiento previo, la actividad de procesamiento posterior y las tareas de políticas de las operaciones de backup, restauración y clonado. Debe colocar los scripts en el directorio de instalación correcto para ejecutar la actividad de preprocesamiento, la actividad de posprocesamiento y las tareas de política de la operación de SnapManager.

Contenido de secuencias de comandos de tareas previas y posteriores

Todos los scripts deben incluir lo siguiente:

- Operaciones específicas (comprobación, descripción y ejecución)
- (Opcional) variables de entorno predefinidas
- Código de manejo de errores específico (código de retorno (rc))

Debe incluir el código de gestión de errores correcto para validar el script.

Puede utilizar los scripts de tareas previas para muchos fines, por ejemplo, limpiar un espacio en disco antes de que se inicie la operación SnapManager. También puede utilizar los scripts posteriores a la tarea, por ejemplo, para calcular si SnapManager tiene espacio en disco suficiente para completar la operación.

Contenido de secuencias de comandos de tareas de directiva

Puede ejecutar el script de directivas sin utilizar operaciones específicas como comprobar, describir y ejecutar. El script incluye las variables de entorno predefinidas (opcionales) y el código de gestión de errores específico.

El script de política se ejecuta antes de las operaciones de backup, restauración y clonado.

Formato admitido

Se puede usar un archivo de comandos con extensión .cmd como script previo y posterior.

Si selecciona el archivo de comandos de shell, la operación SnapManager no responde. Para resolver esto, debe proporcionar el archivo de comandos en el directorio del plugin y volver a ejecutar la operación SnapManager.

Guía de instalación de script

El directorio en el que se instala la secuencia de comandos afecta al modo en que se utiliza. Es posible colocar los scripts en el directorio y ejecutar el script antes o después de que se lleve a cabo la operación de backup, restauración o clonado. Debe colocar el script en el directorio especificado en la tabla y utilizarlo de forma opcional al especificar la operación de backup, restauración o clonado.

Debe asegurarse de que el directorio plugins tenga el permiso ejecutable antes de utilizar los scripts para la operación SnapManager.

Actividad	Backup	Restaurar	Clonar
Preprocesamiento	<default_installation_directory>\plugins\backup\create\pre	<default_installation_directory>\plugins\restore\create\pre	<default_installation_directory>\plugins\clone\create\pre
Procesamiento posterior	<default_installation_directory>\plugins\backup\create\post	<default_installation_directory>\plugins\restore\create\post	<default_installation_directory>\plugins\clone\create\post
Basado en políticas	<default_installation_directory>\plugins\backup\create\policy	<default_installation_directory>\plugins\restore\create\policy	<default_installation_directory>\plugins\clone\create\policy

Ubicación de secuencias de comandos de ejemplo

A continuación se muestran algunos ejemplos de los scripts de tareas previas y posteriores a las tareas para las operaciones de backup y clonado disponibles en la ruta de acceso del directorio de instalación:

- <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

Qué puede cambiar en el script

Si crea un nuevo script, sólo puede cambiar las operaciones describir y ejecutar. Cada script debe contener las siguientes variables: Contexto, tiempo de espera y parámetro.

Las variables descritas en la función describir del script deben declararse al inicio del script. Puede agregar nuevos valores de parámetro en Parameter=() y utilizar los parámetros en la función EXECUTE.

Guión de muestra

A continuación se muestra un script de ejemplo con un código de retorno especificado por el usuario para calcular el espacio en el host SnapManager:

```
@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%
```

Operaciones en scripts de tareas

Las secuencias de comandos de tareas previas o posteriores a las tareas que cree deben seguir una estructura estándar del complemento SnapManager para Oracle.

Las secuencias de comandos de tareas previas y posteriores deben incluir las siguientes operaciones:

- comprobar
- describa
- ejecución

Si alguna de estas operaciones no se especifica en la secuencia de comandos de tareas previas o posteriores, la secuencia de comandos no será válida.

Cuando se ejecuta el comando smo plugin check para los scripts de tareas previas o posteriores, el estado devuelto de los scripts muestra un error (porque el valor de estado devuelto no es cero).

Funcionamiento	Descripción

comprobar	El servidor SnapManager ejecuta el comando plugin.sh -check para garantizar que el sistema tiene permiso de ejecución en los scripts de plugins. También es posible incluir la comprobación de permisos de archivos en el sistema remoto.

describa	El servidor SnapManager ejecuta el comando plugin.sh -describe para obtener información acerca del script y hacer coincidir los elementos proporcionados por el archivo de especificación. El script de un plugin debe contener la siguiente información de descripción:
	
	• SM_PI_NAME: Nombre de script. Debe introducir un valor para este parámetro.
	• SM_PI_DESCRIPTION: Descripción del propósito del script. Debe introducir un valor para este parámetro.
	• SM_PI_CONTEXT: Contexto en el que se debe ejecutar el script, por ejemplo, root u oracle. Debe introducir un valor para este parámetro.
	• SM_PI_TIMEOUT: El tiempo máximo (en milisegundos) que SnapManager debe esperar a que el script complete el procesamiento y finalice la ejecución. Debe introducir un valor para este parámetro.
	• SM_PI_PARAMETER: Uno o varios parámetros personalizados necesarios para que el script del plugin realice el procesamiento. Cada parámetro debe aparecer en una nueva línea de salida e incluir el nombre del parámetro y una descripción. Cuando el script finalice el procesamiento, una variable de entorno proporcionará al script el valor del parámetro.
	
	A continuación se muestra la salida de ejemplo de la secuencia de comandos Followup_Activities.
	
	`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.`

ejecución	El servidor SnapManager ejecuta el comando plugin.sh -execute para iniciar el script y ejecutar el script.

Variables disponibles en los scripts de tareas para la operación de backup

SnapManager proporciona información de contexto en forma de variables de entorno relacionadas con la operación de backup que se realiza. Por ejemplo, el script puede recuperar el nombre del host original, el nombre de la política de retención y la etiqueta del backup.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
SM_OPERATION_ID	Especifica el ID de la operación actual	cadena
SM_PROFILE_NAME	Especifica el nombre del perfil utilizado	cadena
SM_SID	Especifica el identificador del sistema de la base de datos	cadena
SM_HOST	Especifica el nombre de host de la base de datos	cadena
SM_OS_USER	Especifica el propietario del sistema operativo (SO) de la base de datos	cadena
SM_OS_GROUP	Especifica el grupo del sistema operativo de la base de datos	cadena
SM_BACKUP_TYPE	Especifica el tipo de backup (en línea, sin conexión o automático)	cadena
SM_BACKUP_LABEL	Especifica la etiqueta del backup	cadena
SM_BACKUP_ID	Especifica el ID del backup	cadena
SM_BACKUP_RETENCIÓN	Especifica el período de retención	cadena
SM_BACKUP_PROFILE	Especifica el perfil utilizado para esta copia de seguridad	cadena

SM_ALLOW_DATABASE_SHUTDOWN	Especifica si desea iniciar o cerrar la base de datos Si es necesario puede utilizar la opción -force de la interfaz de línea de comandos.	booleano
SM_BACKUP_SCOPE	Especifica el ámbito del backup (completo o parcial)	cadena
SM_TARGET_FILER_NAME	Especifica el nombre del sistema de almacenamiento de destino **Nota:** Si se utiliza más de un sistema de almacenamiento, los nombres de los sistemas de almacenamiento deben separarse con comas.	cadena
SM_TARGET_VOLUME_NAME	Especifica el nombre del volumen de destino **Nota:** el nombre del volumen de destino debe ser prefijado con el nombre del dispositivo de almacenamiento, por ejemplo, SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	cadena
SM_HOST_FILE_SYSTEM	Especifica el sistema de archivos del host	cadena
SM_SNAPSHOT_NAMES	Especifica la lista de instantáneas **Nota:** el nombre de las copias snapshot debe prefijarse con el nombre del sistema de almacenamiento y el nombre del volumen. Los nombres de las copias Snapshot están separados por comas.	matriz de cadenas
SM_ARCHIVE_LOGS_DIRECTORY	Especifica el directorio de registros de archivos **Nota:** Si los registros de archivos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
SM_REDO_LOGS_DIRECTORY	Especifica el directorio de redo logs **Nota:** Si los redo logs se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.	matriz de cadenas

DIRECTORIO_ARCHIVOS_SM_CONTROL	Especifica el directorio de archivos de control **Nota:** Si los archivos de control se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_DATOS_SM	Especifica el directorio de archivos de datos **Nota:** Si los archivos de datos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
definido por el usuario	Especifica parámetros adicionales definidos por el usuario. Los parámetros definidos por el usuario no están disponibles para los plugins que se usan como políticas.	definido por el usuario

Variables disponibles en los scripts de tareas para la operación de restauración

SnapManager proporciona información de contexto en la forma de variables de entorno relacionadas con la operación de restauración que se está realizando. Por ejemplo, el script puede recuperar el nombre del host original y la etiqueta del backup que se restaura.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
SM_OPERATION_ID	Especifica el ID de la operación actual	cadena
SM_PROFILE_NAME	Especifica el nombre del perfil utilizado	cadena
SM_HOST	Especifica el nombre de host de la base de datos	cadena
SM_OS_USER	Especifica el propietario del sistema operativo (SO) de la base de datos	cadena
SM_OS_GROUP	Especifica el grupo del sistema operativo de la base de datos	cadena
SM_BACKUP_TYPE	Especifica el tipo de backup (en línea, sin conexión o automático)	cadena

Variables	Descripción	Formato
SM_BACKUP_LABEL	Especifica la etiqueta de backup	cadena
SM_BACKUP_ID	Especifica el ID del backup	cadena
SM_BACKUP_PROFILE	Especifica el perfil utilizado para el backup	cadena
SM_RECOVERY_TYPE	Especifica la información de configuración de recuperación	cadena
SM_VOLUME_RESTORE_MODE	Especifica la configuración de restauración de volúmenes	cadena
SM_TARGET_FILER_NAME	Especifica el nombre del sistema de almacenamiento de destino **Nota:** Si se utiliza más de un sistema de almacenamiento, los nombres de los sistemas de almacenamiento deben separarse con comas.	cadena
SM_TARGET_VOLUME_NAME	Especifica el nombre del volumen de destino **Nota:** el nombre del volumen de destino debe ser prefijado con el nombre del dispositivo de almacenamiento, por ejemplo, SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	cadena
SM_HOST_FILE_SYSTEM	Especifica el sistema de archivos del host	cadena
SM_SNAPSHOT_NAMES	Especifica la lista de instantáneas **Nota:** el nombre de las copias snapshot debe prefijarse con el nombre del sistema de almacenamiento y el nombre del volumen. Los nombres de las copias Snapshot están separados por comas.	matriz de cadenas
SM_ARCHIVE_LOGS_DIRECTORY	Especifica el directorio de registros de archivos **Nota:** Si los registros de archivos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas

Variables	Descripción	Formato
SM_REDO_LOGS_DIRECTORY	Especifica el directorio de redo logs **Nota:** Si los redo logs se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_SM_CONTROL	Especifica el directorio de archivos de control **Nota:** Si los archivos de control se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas
DIRECTORIO_ARCHIVOS_DATOS_SM	Especifica el directorio de archivos de datos **Nota:** Si los archivos de datos se encuentran en más de un directorio, los nombres de esos directorios se separan por comas.	matriz de cadenas

Variables disponibles en los scripts de tareas para la operación de clonado

SnapManager proporciona información de contexto en forma de variables de entorno relacionadas con la operación de clonado que se realiza. Por ejemplo, el script puede recuperar el nombre del host original, el nombre de la base de datos clonada y la etiqueta del backup.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
SM_ORIGINAL_SID	SID de la base de datos original	cadena
SM_ORIGINAL_HOST	Nombre de host asociado con la base de datos original	cadena
SM_ORIGINAL_OS_USER	Propietario del sistema operativo de la base de datos original	cadena
SM_ORIGINAL_OS_GROUP	Grupo del sistema operativo de la base de datos original	cadena
SM_TARGET_SID	SID de la base de datos del clon	cadena
SM_TARGET_HOST	Nombre del host asociado con la base de datos del clon	cadena

SM_TARGET_OS_USER	Propietario del sistema operativo de la base de datos clonada	cadena
SM_TARGET_OS_GROUP	Grupo del sistema operativo de la base de datos clonada	cadena
SM_TARGET_DB_PORT	Puerto de la base de datos de destino	entero
SM_TARGET_GLOBAL_DB_NAME	Nombre de la base de datos global de la base de datos de destino	cadena
SM_BACKUP_LABEL	Etiqueta del backup utilizado para el clon	cadena

Error al manejar en scripts personalizados

SnapManager procesa la secuencia de comandos personalizada según los códigos de retorno específicos. Por ejemplo, si el script personalizado devuelve el valor 0, 1, 2 o 3, SnapManager continúa con el proceso de clonado. El código de retorno también influye en el modo en que SnapManager procesa y devuelve la salida estándar de la ejecución de la secuencia de comandos.

Código de retorno	Descripción	Continúe procesando la operación
0	El script se ha completado correctamente.	Sí
1	El script se ha completado correctamente, con mensajes informativos.	Sí
2	La secuencia de comandos se ha completado, pero incluye advertencias	Sí
3	La secuencia de comandos falla, pero la operación continúa.	Sí
4 o >4	El script falla y la operación se detiene.	No

Ver scripts de plugin de muestra

SnapManager incluye scripts que puede utilizar como ejemplos para crear sus propios scripts o como base para sus scripts personalizados.

Puede encontrar los scripts de plugins de muestra en la siguiente ubicación:

- <default_install_directory>\plugins\examples\backup\create
- <default_install_directory>\plugins\examples\clone\create
- <default_install_directory>\plugins\windows\examples\backup\create\post

El directorio que contiene los scripts de plug-in de ejemplo incluye los siguientes subdirectorios:

- Policy: Contiene scripts que, cuando se configuran, ejecutan siempre en la operación de clonado.
- Pre: Contiene scripts que, cuando se configuran, se ejecutan antes de la operación de clonado.
- Post: Contiene scripts que, cuando se configuran, se ejecutan después de la operación de clonado.

En la siguiente tabla se describen los scripts de ejemplo:

Nombre de script	Descripción	Tipo de script
validate_sid.sh	Contiene comprobaciones adicionales al SID utilizado en el sistema de destino. La secuencia de comandos comprueba que el SID tenga las siguientes características: • Contiene tres caracteres alfanuméricos • Comienza con una letra	Política
cleanup.sh	Borra el sistema de destino de modo que esté listo para almacenar el clon recién creado. Conserva o elimina archivos y directorios en función de la necesidad.	Pretask
Mirror_the_backup.cmd	Refleja los volúmenes después de que la operación de backup se produzca en un entorno de Windows cuando se utiliza Data ONTAP en 7-Mode.	Postarea
Vault_the_backup.cmd	Almacena los qtrees después de que la operación de backup se produzca en un entorno Windows cuando utiliza la versión de Data ONTAP en 7-Mode.	Postarea

Mirror_the_backup_CDOT.cmd	Refleja los volúmenes después de que la operación de backup se produzca en un entorno Windows cuando se utiliza Clustered Data ONTAP.	Postarea
Vault_the_backup_CDOT.cmd	Almacena los qtrees después de que se realice la operación de backup en un entorno Windows cuando utiliza Clustered Data ONTAP.	Postarea

Los scripts suministrados con SnapManager utilizan el shell BASH de forma predeterminada. Debe asegurarse de que el soporte para el shell BASH está instalado en su sistema operativo antes de intentar ejecutar cualquiera de los scripts de ejemplo.

1. Para verificar que está usando el shell BASH, introduzca el siguiente comando en el símbolo del sistema: Bash

   Si no ve un error, el shell BASH está funcionando correctamente.

   De forma alternativa, puede introducir el comando qu-bash en el símbolo del sistema.

2. Busque el script en el siguiente directorio:

   <installdir>\plugins\examples\clone\create

3. Abra el script en un editor de secuencia de comandos como vi.

Guión de muestra

El siguiente script personalizado de muestra valida los nombres de SID de base de datos y evita que los nombres no válidos se usen en la base de datos clonada. Incluye tres operaciones (comprobación, descripción y ejecución), a las que se llama después de ejecutar el script. La secuencia de comandos también incluye el manejo de mensajes de error con los códigos 0, 4 y >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%
```

Creación de scripts de tareas

Es posible crear los scripts de tareas previas, posteriores a tareas y de políticas para operaciones de backup, restauración y clonado, escribir el script e incluir las variables de entorno predefinidas en los parámetros. Es posible crear un nuevo script o modificar uno de los scripts de ejemplo de SnapManager.

Antes de comenzar a crear el script, asegúrese de lo siguiente:

- Es necesario estructurar el script de un modo determinado para que se ejecute en el contexto de una operación SnapManager.
- Debe crear el script en función de las operaciones esperadas, los parámetros de entrada disponibles y las convenciones de código de devolución.
- Debe incluir mensajes de registro y redirigir los mensajes a archivos de registro definidos por el usuario.

  a. Cree la secuencia de comandos de la tarea personalizando la secuencia de comandos de ejemplo.

     Realice lo siguiente:

     i. Busque un script de ejemplo en el siguiente directorio de instalación:

        <default_install_directory>\plugins\examples\backup\create

     <default_install_directory>\plugins\examples\clone\create

     i. Abra el script en el editor de secuencia de comandos.
     ii. Guarde el script con un nombre diferente.

  b. Modifique las funciones, variables y parámetros según sea necesario.
  c. Guarde el script en uno de los siguientes directorios:

     Secuencias de comandos de operaciones de copia de seguridad

     - <default_install_directory>\plugins\backup\create\pre: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.

- <default_install_directory>\plugins\backup\create\post: Ejecuta el script después de que se realice la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>\plugins\backup\create\policy: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio. **Restaurar secuencias de comandos de operación**
- <default_install_directory>\plugins\restore\create\pre: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>\plugins\restore\create\post: Ejecuta el script después de que se realice la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>\plugins\restore\create\policy: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio. **Clonar secuencias de comandos**
- <default_install_directory>\plugins\clone\create\pre: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>\plugins\clone\create\post: Ejecuta el script después de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- <default_install_directory>\plugins\clone\create\policy: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio.

Almacenamiento de los scripts de tareas

Debe almacenar los scripts de tareas previas, posteriores a tareas y de políticas en un directorio especificado en el servidor de destino donde se crearán los backups o clones. Para la operación de restauración, los scripts deben colocarse en el directorio especificado en el servidor de destino donde se desea restaurar el backup.

1. Cree el script.
2. Guarde el script en una de las siguientes ubicaciones:

Para la operación de copia de seguridad

Directorio	Descripción
<default_install_directory >\plugins\backup\create\policy	Los scripts de políticas se ejecutan antes de las operaciones de backup.
<default_install_directory >\plugins\backup\create\pre	Los scripts de preprocesamiento ejecutan el antes de las operaciones de backup.
<default_install_directory >\plugins\backup\create\pre	Los scripts de procesamiento posterior se ejecutan después de las operaciones de backup.

Para la operación de restauración

Directorio	Descripción

<default_install_directory >\plugins\restore\create\policy	Los scripts de políticas se ejecutan antes de las operaciones de restauración.
<default_install_directory >\plugins\restore\create\pre	Las secuencias de comandos de preprocesamiento se ejecutan antes de las operaciones de restauración.
<default_install_directory >\plugins\restore\create\post	Los scripts posteriores al procesamiento se ejecutan después de las operaciones de restauración.

Para la operación de clonación

Directorio	Descripción
<default_install_directory >\plugins\clone\create\policy	Los scripts de políticas se ejecutan antes de las operaciones de clonado.
<default_install_directory >\plugins\clone\create\pre	Los scripts de procesamiento previo se ejecutan antes de las operaciones de clonado.
<default_install_directory >\plugins\clone\create\post	Los scripts de procesamiento posterior se ejecutan después de las operaciones de clonado.

Verificar la instalación de los scripts de los plugins

SnapManager le permite instalar y utilizar scripts personalizados para realizar diversas operaciones. SnapManager proporciona plugins para las operaciones de backup, restauración y clonado, que puede usar para automatizar sus scripts personalizados antes y después de las operaciones de backup, restauración y clonado.

1. Introduzca el siguiente comando:

   comprobación del complemento de smo -osaccount nombre de usuario de la base de datos del sistema operativo

   Si no se proporciona la opción -osaccount, la verificación de la instalación del script de plugin tiene lugar para el administrador en lugar de para el usuario especificado.

   El siguiente resultado indica que las secuencias de comandos policy 1, pre-plugin1 y pre-plugin2 se han instalado correctamente. Sin embargo, la secuencia de comandos post-plugin1 no funciona.

```
            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.
```

Creación de un archivo de especificación de tareas

Puede crear los archivos de especificación de tareas mediante la interfaz gráfica de usuario (GUI), la interfaz de línea de comandos (CLI) o un editor de texto. Estos archivos se utilizan para realizar un procesamiento previo o la actividad de posprocesamiento de las operaciones de backup, restauración o clonado.

1. Cree un archivo de especificación de tareas mediante GUI, CLI o un editor de texto.

   Puede crear el archivo de especificación según la estructura del siguiente archivo de especificación de tareas de ejemplo:

```
<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. Introduzca el nombre del script.
3. Introduzca el nombre del parámetro y el valor asignado al parámetro.
4. Guarde el archivo XML en el directorio de instalación correcto.

Ejemplo de especificación de tarea

```
  <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>
```

Realizar operaciones de backup, restauración y clonado mediante scripts previos y posteriores

Puede usar su propio script para iniciar una operación de backup, restauración o clonado. SnapManager muestra una página Task-abling en el asistente Backup Create, el asistente Restore or Recover o el asistente Clone Create, donde puede seleccionar el script y proporcionar valores a los parámetros que requiera el script.

- Instale los scripts de los plugins en la ubicación correcta de instalación de SnapManager.
- Compruebe que los complementos estén instalados correctamente con el comando smsap plugin check.

- Asegúrese de que está utilizando el shell BASH.

En la interfaz de línea de comandos (CLI), enumere el nombre del script, seleccione los parámetros y configure los valores.

1. Para verificar que está usando el shell BASH, introduzca el siguiente comando en el símbolo del sistema:bash

   Como alternativa, puede introducir el comando cuál-bash en el símbolo del sistema y utilizar el resultado del comando como parámetro de inicio del script.

   El shell BASH funciona correctamente si no ve un error.

2. Para la operación de backup, introduzca la opción -taskspec y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un preprocesamiento o una actividad de posprocesamiento que se debe realizar antes o después de la operación de backup: smo backup create -profile_name {[-full {-online | -offline | -auto} [-retenga {-hora | [-diaria | -semanal | -mensual | -unlimited}] [-verify] | [-data [-lablothora archivos [archivos] | [-tablespaces [-commentation]] [-compointing] | -retain] [-backup-destinpath1 [,[path2]]] [-exclude-destinpath1 [,path2]]] [-prunogs {-all | -untilSCNuntilSCN | -before {-dateyy-MM-dd HH:mm:ss | -months | -days | -weeks | -hours} -spuni] -despruni-toverbowune] -toverbowent-backup [-pruni]

   Si se produce un error en la operación del plugin de backup, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

3. Para la operación de restauración de backup, introduzca la opción -taskspec y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un preprocesamiento o una actividad de posprocesamiento que debe tener lugar antes o después de la operación de restauración: backup restore -profileprofile_name {-lableared <label> | -rage <id>} {-fastute <files>|-tablecarance <tablespaces> | -complete | -controlfiles} [-recover {-alllogs | -nologs | -until <until>}][-<restorespec>] [-<taskspec>] [-verify][-force] | restore-povered-povered | -rback up | -rback up]

   Si se produce un error en la operación del plugin de restauración, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

4. Para la operación de creación de clones, introduzca la opción -taskspec y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un procesamiento previo o una actividad de procesamiento posterior que debe tener lugar antes o después de la operación de clonado: crear -profileprofile_name {-backup-labelbackup_name | -backup-<backup-id>| -current} -newsidnew_sid -clonespecepath_to_labonespecesfichero [-reserveprofile_<yes, no, inherit>] [-<host>] [-<label>] [-<comment>] -<taskspec>_]

   Si se produce un error en la operación del plugin de clonado, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

Ejemplo de creación de una copia de seguridad utilizando el archivo XML de especificación de tareas

```
smo backup create -profile SALES1 -full -online -taskspec
sales1_taskspec.xml -force -verify
```

Actualizar el nombre del sistema de almacenamiento y el nombre de host de la base de datos de destino asociados con un perfil

Con SnapManager 3.3 o versiones posteriores, es posible actualizar el nombre de host del sistema de almacenamiento o la dirección del sistema de almacenamiento, así como el nombre de host de la base de datos de destino asociado con un perfil de SnapManager.

Actualizar el nombre del sistema de almacenamiento asociado con un perfil

A partir de la versión 3.3 de SnapManager, es posible actualizar el nombre de host o la dirección IP de un sistema de almacenamiento asociado con un perfil.

Debe asegurarse de lo siguiente:

- El perfil tiene al menos una copia de seguridad.

  Si el perfil no tiene backup, no es necesario actualizar el nombre del sistema de almacenamiento para ese perfil.

- No se está ejecutando ninguna operación para el perfil.

Puede actualizar el nombre o la dirección IP del sistema de almacenamiento mediante la interfaz de línea de comandos (CLI) de SnapManager. Mientras se actualiza el nombre del sistema de almacenamiento, se actualizan los metadatos almacenados únicamente en la base de datos del repositorio. Después de cambiar el nombre del sistema de almacenamiento, puede realizar todas las operaciones de SnapManager como antes.

> No se puede cambiar el nombre del sistema de almacenamiento mediante la interfaz gráfica de usuario (GUI) de SnapManager.

Debe asegurarse de que haya copias Snapshot disponibles en el nuevo sistema de almacenamiento. SnapManager no verifica la existencia de las copias Snapshot en el sistema de almacenamiento.

Sin embargo, debe recordar lo siguiente al realizar la actualización y reversión del host después de cambiar el nombre del sistema de almacenamiento:

- Si va a realizar una actualización gradual del host después de cambiar el nombre del sistema de almacenamiento, debe actualizar el perfil con el nuevo nombre del sistema de almacenamiento.
- Si va a revertir el host después de cambiar el nombre del sistema de almacenamiento, debe asegurarse de cambiar el nombre del sistema de almacenamiento a su nombre anterior para poder utilizar los perfiles, los backups y los clones del sistema de almacenamiento anterior para ejecutar operaciones de SnapManager.
  a. Introduzca el siguiente comando: smo Storage rename -profileprofile-oldnamedold_Storage_name -newnamenew_Storage_name [quiet | -verbose]

Si desea…	Realice lo siguiente…

Actualice el nombre del sistema de almacenamiento asociado a un perfil	Especifique la opción -profile.
Actualice el nombre o la dirección IP del sistema de almacenamiento asociados a un perfil	Especifique las siguientes opciones y variables: • -Oldnamedold_Storage_name es el nombre de host o la dirección IP del sistema de almacenamiento. • -Newnamenew_Storage_name es el nombre de host o la dirección IP del sistema de almacenamiento.

En el ejemplo siguiente se muestra el nombre del sistema de almacenamiento que se está actualizando:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Ver una lista de sistemas de almacenamiento asociados a un perfil

Puede ver una lista de los sistemas de almacenamiento asociados con un perfil en particular.

La lista muestra los nombres de los sistemas de almacenamiento asociados con el perfil en particular.

> Si no hay backups disponibles para el perfil, no puede ver el nombre del sistema de almacenamiento asociado con el perfil.

1. Para mostrar la información de los sistemas de almacenamiento asociados con un perfil determinado, escriba este comando: smo Storage list -profileprofile [-quiet | -verbose]

Ejemplo

```
smo storage list -profile mjubllian
```

```
Sample Output:
Storage Controllers
--------------------
STCO1110-RTP07OLD
```

Actualizar el nombre de host de la base de datos de destino asociado a un perfil

SnapManager (3.2 o posterior) para Oracle ofrece la posibilidad de actualizar el nombre de host de la base de datos de destino en el perfil de SnapManager.

- El directorio inicial del usuario local debe tener en cuenta las asignaciones de perfil a repositorio.
- Se deben cerrar las sesiones de la interfaz gráfica de usuario (GUI) de SnapManager.

Puede actualizar el perfil con el nuevo nombre de host únicamente mediante la CLI.

Escenarios no admitidos para cambiar el nombre de host de la base de datos de destino en Profile

Las siguientes situaciones no son compatibles para cambiar el nombre de host de la base de datos de destino en el perfil:

- Cambiar el nombre de host de la base de datos de destino mediante la interfaz gráfica de usuario de SnapManager
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil
- Actualizar varios perfiles para un nuevo nombre de host de base de datos de destino ejecutando un solo comando
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager

> Después de actualizar el nombre de host de la base de datos de destino en el perfil, solo se cambia el nombre de host de la base de datos de destino. Se conservan todos los demás parámetros de configuración establecidos en el perfil.

Después de actualizar el nombre de host de la base de datos de destino, no se puede eliminar ni desmontar el backup si el clon o el backup montado no están disponibles en el nuevo host. En tales situaciones, ejecutar las operaciones de SnapManager desde el host nuevo conlleva el fallo y las entradas obsoletas del host anterior. Para realizar operaciones de SnapManager, debe revertir al nombre de host anterior mediante la actualización de perfil.

1. Introduzca el siguiente comando: smo profile update -profileprofile [-profile-passwordprofile_password][-database-dbnamedb_dbname-hostdB_host [-siddb_sid] [-login-usernamedb_username [-passb_password-directnb] [-directnod_email]-stain]-directntn]-directnend] [-want-want]-want-wonseisseisseissep]-want]-want-want-want] [-wonseissein]-want-want-want-want-wonsmand] [-wonman]-want-wonset]-wonset]-wonset]-wonman]-wonset [-wonman]-wonman]-wonseisseisseisseisseisseisseisseisseisseisseisseisseissein] [-wonman]-wonman]-wonman

   Las demás opciones para este comando son las siguientes:

   [-force] [-noprompt]

Si desea…	Realice lo siguiente…
Cambiar el nombre de host de la base de datos de destino	Especifique -hostnew_dB_host

2. Para ver el nombre de host de la base de datos de destino del perfil, introduzca el siguiente comando: smo profile show

Mantener el historial de operaciones de SnapManager

SnapManager para Oracle le permite mantener el historial de operaciones de

SnapManager asociadas con un único perfil o múltiples perfiles. Puede mantener el historial desde la interfaz de línea de comandos (CLI) de SnapManager o desde la interfaz gráfica de usuario (GUI). Puede ver el historial de las operaciones como un informe y utilizar el informe para fines de cumplimiento de auditoría.

Puede mantener el historial de las siguientes operaciones de SnapManager:

- Crear backup
- Verificación de backup
- Restauración de backup
- Clone create

La información del historial de las operaciones de SnapManager se mantiene en función de la retención. Puede configurar diferentes clases de retención para cada una de las operaciones de SnapManager admitidas.

A continuación se enumeran algunas clases de retención que puede asignar:

- Número de días
- Número de semanas
- Número de meses
- Cantidad de operaciones

Según la retención, SnapManager purga el historial automáticamente. También puede purgar manualmente el historial de las operaciones de SnapManager. Si elimina o destruye el perfil, se eliminará toda la información del historial asociada con el perfil.

> Después de revertir el host, no se pueden ver los detalles del historial ni se pueden realizar operaciones relacionadas con el historial asociadas con el perfil que se haya configurado para el mantenimiento del historial.

Configurar el historial de funcionamiento de SnapManager

SnapManager para Oracle le permite mantener el historial de operación de SnapManager desde la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager. Puede ver el historial de la operación SnapManager como un informe.

1. Para configurar el historial de la operación de SnapManager, introduzca el siguiente comando: smo history set -profile {-name, profile_name [profile_name1, profile_name2] | -all-repository [-passwwordrepo_password] -usernamerepo_username-namerepo_dbname-strepo_host -opertain_operation_weeklog | -weeklog_operation_weeklog_weeklog_1} -weekly} -weeklog_operation_weeklog_operation_weeklog_weeklog_weekly} -weeklog_operation_weeklog_weeklog_weeklog_weeklog_weekly}

```
        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
```

Ver una lista del historial de operaciones de SnapManager

Puede ver el historial de todas las operaciones de SnapManager específicas o como un informe de acuerdo con la configuración de retención.

1. Para ver una lista de operaciones de historial de SnapManager, introduzca el siguiente comando: lista de historial de smo -profile {-name, nombre_de_perfil [nombre_perfil_1,perfil_nombre2] | -all-repositorio-login [-passwwordrepo_password] -usernamerpo_nombre_nombre_host-operation [_operation]-operation_todo_1}

Ver el historial detallado de una operación específica asociada a un perfil

Es posible ver el historial detallado de una operación SnapManager específica asociada con un perfil.

1. Para mostrar información detallada del historial de una operación de SnapManager específica asociada con un perfil, escriba el siguiente comando: `smo history operation-show -profileprofile_name {-labellabel | -ididd} [-quiet | -verbose]`

Eliminando historial de operación de SnapManager

Puede eliminar el historial de la operación SnapManager si ya no se necesitan los detalles del historial.

1. Para eliminar el historial de la operación SnapManager, introduzca el siguiente comando: smo history purge -profile {-name, profile_name1_name1, profile_name2] | all-repository-login [-passwdrepo_password] -usernamerepo_username-namerepo_dbname-hotname-nombreelpo_operation [-operation] -all-operation]

Eliminar la configuración del historial asociada a un único perfil o a varios perfiles

SnapManager permite eliminar la configuración del historial de una operación SnapManager. Esta operación purga toda la información del historial asociada con un único perfil o múltiples perfiles.

1. Para eliminar el historial de operaciones de SnapManager asociadas con un único perfil o varios perfiles, introduzca el siguiente comando: SMO history remove -profile {-name, profile_name [profile_name1, profile_name2] | all-repository [-passwddrepo_password] -usernamerepo_username-dberpo_nombredepo -operation [_renamepo]_operation]

Ver detalles de configuración del historial de SnapManager

Puede ver la configuración del historial de un único perfil.

La operación del historial de SnapManager muestra la siguiente información para cada perfil:

- Nombre de la operación
- Clase de retención
- Recuento de retención
  a. Para mostrar información acerca de la operación del historial de SnapManager de un perfil específico, escriba el siguiente comando: smo history show -profileprofile_name

Referencia de comandos de SnapManager para Oracle

La referencia del comando SnapManager incluye la sintaxis de uso, las opciones, los parámetros y los argumentos que debe proporcionar con los comandos, junto con ejemplos.

Los siguientes problemas se aplican al uso de comandos:

- Los comandos distinguen mayúsculas de minúsculas.
- SnapManager acepta hasta 200 caracteres y etiquetas de hasta 80 caracteres.
- Si el shell del host limita el número de caracteres que pueden aparecer en una línea de comandos, puede utilizar el comando cmdfile.
- No utilice espacios en nombres de perfiles ni nombres de etiquetas.
- En la especificación del clon, no utilice espacios en la ubicación del clon.

SnapManager puede mostrar tres niveles de mensajes en la consola:

- Mensajes de error
- Mensajes de advertencia
- Mensajes informativos

Puede especificar cómo desea que se muestren los mensajes. Si no especifica nada, SnapManager solo muestra mensajes de error y advertencias en la consola. Para controlar la cantidad de salida que SnapManager muestra en la consola, utilice una de las siguientes opciones de línea de comandos:

- -Quiet: Sólo muestra mensajes de error en la consola.
- -Verbose: Muestra mensajes de error, advertencia y informativos a la consola.

> Independientemente del comportamiento predeterminado o del nivel de detalle especificado para la pantalla, SnapManager siempre escribe todos los tipos de mensaje en los archivos de registro.

El comando smo_Server restart

Este comando reinicia el servidor host SnapManager y se introduce como root.

Sintaxis

```
        smo_server restart
[-quiet | -verbose]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Comando de ejemplo

En el ejemplo siguiente se reinicia el servidor host.

```
smo_server restart
```

El comando start smo_Server

Este comando inicia el servidor host que ejecuta el software SnapManager para Oracle.

Sintaxis

```
        smo_server start
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Comando de ejemplo

En el ejemplo siguiente se inicia el servidor host.

```
smo_server start
SMO-17100: SnapManager Server started on secure port 25204 with PID 11250
```

El comando de estado del servidor smo_server

Puede ejecutar el comando status de smo_Server para ver el estado del servidor host

SnapManager.

Sintaxis

```
        smo_server status
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Ejemplo

En el siguiente ejemplo, se muestra el estado del servidor de host:

```
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.
```

El comando smo_Server stop

Este comando detiene el servidor host de SnapManager y se introduce en la raíz.

Sintaxis

```
        smo_server stop
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

Comando de ejemplo

En el ejemplo siguiente se utiliza el comando smo_Server stop.

```
smo_server stop
```

El comando smo backup create

El comando backup create permite crear backups de base de datos en uno o varios sistemas de almacenamiento.

Sintaxis

> Antes de ejecutar este comando, debe crear un perfil de base de datos mediante el comando profile create.

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos de la que desea realizar backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-opción automática**

  Si la base de datos está en estado montado o sin conexión, SnapManager realiza un backup sin conexión.

Si la base de datos está en estado abierto o en línea, SnapManager realiza un backup en línea. Si se utiliza la opción -force con la opción -offline, SnapManager fuerza un backup sin conexión aunque la base de datos esté actualmente en línea.

- **-opción en línea**

  Especifica un backup de base de datos en línea.

  - Si la instancia local está en estado de apagado y al menos una instancia está en estado abierto, puede utilizar la opción -force para cambiar la instancia local al estado montado.
  - Si ninguna instancia está en estado abierto, puede utilizar la opción -force para cambiar la instancia local al estado abierto.

- **-opción sin conexión**

  Especifica una copia de seguridad sin conexión mientras la base de datos está en estado de apagado. Si la base de datos está en estado abierto o montado, el backup genera errores. Si se utiliza la opción -force, SnapManager intenta modificar el estado de la base de datos para cerrar la base de datos con el fin de realizar una copia de seguridad sin conexión.

- **-opción completa**

  Realiza un backup de toda la base de datos. Esto incluye todos los datos, registros archivados y archivos de control. Se realiza una copia de seguridad de los redo logs archivados y de los archivos de control, independientemente del tipo de copia de seguridad que realice. Si se desea realizar un backup solo de una parte de la base de datos, se deben utilizar la opción -files o -tablespaces.

- **-opción de datos**

  Especifica los archivos de datos.

- **-lista de archivos**

  Realiza un backup solo de los archivos de datos especificados, además de los archivos de registro y control archivados. Separe la lista de nombres de archivo con espacios. Si la base de datos se encuentra en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-tablespaces**

  Realiza un backup solo de los espacios de tablas de la base de datos especificados, además de los archivos de registro y control archivados. Separe los nombres de tablespace con espacios. Si la base de datos se encuentra en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- * etiqueta*

  Especifica un nombre opcional para este backup. Este nombre debe ser único dentro del perfil. El nombre puede contener letras, números, guiones bajos (_) y guiones (-). No puede comenzar con un guión. Si no se especifica una etiqueta, SnapManager crea una etiqueta predeterminada en el formato scope_type_date:

  - El ámbito es F indicar un backup completo o P para indicar un backup parcial.
  - El tipo es C para indicar una copia de seguridad sin conexión (en frío), H para indicar una copia de seguridad en línea (activa) o A para indicar una copia de seguridad automática, por ejemplo,

P_A_20081010060037IST.

- Fecha es el año, el mes, el día y la hora de la copia de seguridad.

  SnapManager se usa un reloj de 24 horas.

Por ejemplo, si realizó un backup completo con la base de datos sin conexión el 16 de enero de 2007, a las 5:45:16 Hora estándar del este, SnapManager crearía la etiqueta F_C_20070116174516EST.

- **-cadena de comentario**

  Especifica un comentario opcional para describir esta copia de seguridad. La cadena debe escribirse entre comillas simples (').

  > Algunos vaciados despegan las comillas. En este caso, se debe incluir la comillas con una barra diagonal inversa (\). Por ejemplo, es posible que deba introducir la siguiente información: `\' this is a comment\'`.

- **-verificar opción**

  Verifica que los archivos de la copia de seguridad no están dañados ejecutando la utilidad oracle dbv.

  > Si se especifica la opción -Verify, la operación de backup no se completará hasta que finalice la operación de verificación.

- **-opción de fuerza**

  Fuerza un cambio de estado si la base de datos no está en el estado correcto. Por ejemplo, SnapManager puede cambiar el estado de la base de datos de en línea a sin conexión, según el tipo de backup especificado y el estado en el que está la base de datos.

  - Si la instancia local está en estado de apagado y al menos una instancia está en estado abierto, el uso de la opción -force cambia la instancia local al estado montado.
  - Si ninguna instancia está en el estado abierto, con la opción -force , la instancia local cambia al estado abierto.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

- **-retener { -hora | -diario | -semanal | -mensual | -ilimitado}**

  Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si no se especifica la opción -retain, la clase de retención predeterminada es la opción -Hourly. Para retener las copias de seguridad para siempre, utilice la opción -Unlimited. La opción -Unlimited hace que el backup no sea apto para que lo elimine la política de retención.

- **-archivelogs opción**

  Crea un backup de registro de archivos.

- **-backup-más extraño path1, [, [path2]]**

  Especifica los destinos de registros de archivos que se incluirán en el backup para el backup de registros de archivos.

- **-exclude-más extraño path1, [, [path2]]**

  Especifica los destinos de registro de archivos que se excluirán de la copia de seguridad.

- **-prunelogs {-all | -until-scnuntil-scn | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-meses | -días | -semanas | -horas}**

  Elimina los archivos de registro de archivos de los destinos de registro de archivos según las opciones proporcionadas al crear un backup. La opción -all elimina todos los archivos de registro de archivos de los destinos de registro de archivos. La opción -until-scn elimina los archivos de registro de archivos hasta que se especifique un número de cambio de sistema (SCN). La opción -until-date elimina los archivos de registro de archivos hasta el periodo de tiempo especificado. La opción -before elimina los archivos de registro de archivos antes del periodo de tiempo especificado (días, meses, semanas, horas).

- **-prune-dest prune_dest1,prune_dest2**

  Elimina los archivos de registro de archivos de los destinos de registro de archivos mientras se crea el backup.

- **-tasktaskspec**

  Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Se debe proporcionar la ruta completa del archivo XML al proporcionar la opción -taskspec .

- **-opción de volcado**

  Recoge los archivos de volcado después de una operación de backup de base de datos con errores o realizada correctamente.

Comando de ejemplo

El siguiente comando crea un backup completo en línea, crea un backup en el almacenamiento secundario y establece la política de retención en diaria:

```
smo backup create -profile SALES1 -full -online
-label full_backup_sales_May -profile SALESDB -force -retain -daily
Operation Id [8abc01ec0e79356d010e793581f70001] succeeded.
```

Información relacionada

Creación de backups de la base de datos

El comando smo profile create

El comando smo backup delete

Puede ejecutar el comando backup delete para quitar backups que no se quitan automáticamente, como los backups que se usaron para crear un clon o backups que generaron errores. Puede eliminar backups retenidos de forma ilimitada sin cambiar la clase de retención.

Sintaxis

```
        smo backup delete
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la base de datos asociada con el backup que desea quitar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Especifica la copia de seguridad con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Especifica el backup con la etiqueta especificada. Opcionalmente, especifique el alcance del backup como archivo de datos o registro de archivo.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-todo**

  Especifica todos los backups. Para eliminar solo los backups especificados, use la opción -id o -label.

- **-dump**

  Recopila los archivos de volcado después de una operación de eliminación de backup realizada correctamente o con errores.

- **-fuerza**

Fuerza la eliminación del backup. SnapManager elimina el backup incluso si hay problemas para liberar los recursos asociados con el backup. Por ejemplo, si el backup se catalogó con Oracle Recovery Manager (RMAN), pero la base de datos de RMAN ya no existe, incluido -force elimina el backup aunque no pueda conectarse con RMAN.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se elimina el backup:

```
smo backup delete -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Información relacionada

Eliminar backups

El comando smo profile create

El comando smo profile update

El comando libre de backup de smo

Puede ejecutar el comando backup free para liberar las copias Snapshot de los backups sin eliminar los metadatos de backup del repositorio.

Sintaxis

```
        smo backup free
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil asociado al backup que desea liberar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Especifica los recursos del backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup. Incluye la opción -verbose para mostrar los ID de backup.

- * etiqueta*

  Especifica el backup con la etiqueta especificada.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-todo**

  Especifica todos los backups. Para eliminar los backups especificados, use la opción -id o -label.

- **-fuerza**

  Fuerza la eliminación de las copias snapshot.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se libera el backup:

```
smo backup free -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Información relacionada

Liberando backups

El comando smo backup list

Puede ejecutar el comando backup list para ver información sobre los backups de un perfil, incluida la información sobre la clase de retención y el estado de protección.

Sintaxis

```
        smo backup list
-profile profile_name
-delimiter character
[-data | -archivelogs | -all]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea mostrar las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- * carácter delimitador*

  Muestra cada fila en una línea diferente. Los atributos de la fila están separados por el carácter especificado.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola. Incluye la opción -verbose para mostrar los ID de backup.

Ejemplo

En el ejemplo siguiente se enumeran las copias de seguridad del perfil SALES1:

```
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
```

Información relacionada

Ver una lista de backups

El comando de montaje de backup de smo

Puede ejecutar el comando backup Mount para montar un backup y realizar una operación de recuperación con una herramienta externa.

Sintaxis

```
        smo backup mount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
[-host  host]

\[-dump\]
[-quiet | -verbose]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil asociado con el backup que desea montar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Monta la copia de seguridad con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Monta la copia de seguridad con la etiqueta especificada.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-host**

  Especifica el host en el que desea montar el backup.

- **-dump**

  Recopila los archivos de volcado después de la operación de montaje correcta o con errores.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

> Debe utilizar este comando sólo si utiliza una herramienta externa como Oracle Recovery Manager (RMAN). SnapManager se encarga automáticamente del montaje de backups si se utiliza el comando smo backup restore para restaurar el backup. Este comando muestra una lista, que muestra las rutas donde se han montado las copias Snapshot. Esta lista solo se muestra cuando se especifica la opción -verbose.

Ejemplo

En el ejemplo siguiente se monta la copia de seguridad:

```
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
```

Información relacionada

Montar backups

El comando smo backup restore

Se puede ejecutar el comando backup restore para restaurar backups de una base de datos o una parte de una base de datos y, opcionalmente, recuperar la información de la base de datos.

Sintaxis

```
        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 \[, path2\]\]
\[-taskspec taskspec\]
\[-dump\]
\[-force\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la base de datos que desea restaurar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre de etiqueta**

  Restaura el backup con la etiqueta especificada.

- **-id guid**

  Restaura el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- **Elija todos los archivos o especificados**

  De manera opcional, puede utilizar una de las siguientes opciones:

  - -Complete: Restaura todos los archivos de datos de la copia de seguridad.
  - -Tableslist: Restaura sólo los tablespaces especificados a partir de la copia de seguridad.

    Debe utilizar espacios para separar los nombres en la lista.

  - -Fileslist: Restaura sólo los archivos de datos especificados de la copia de seguridad.

    Debe utilizar espacios para separar los nombres en la lista. Si la base de datos se está ejecutando, SnapManager garantiza que el tablespace que contiene los archivos esté sin conexión.

- **-controlfiles**

  Restaura los archivos de control. SnapManager permite restaurar archivos de control junto con los

archivos de datos de los backups en una única operación. La opción -controlfiles es independiente de otros parámetros de alcance de restauración, como -complete, -tablespaces y -files.

- **-recover**

  Recupera la base de datos después de restaurarla. También debe especificar el punto en el que desea que SnapManager recupere la base de datos mediante una de las siguientes opciones:

  - -Nologs: Recupera la base de datos al momento de la copia de seguridad y no aplica registros.

    Este parámetro se puede usar para backups en línea o sin conexión.

  - -Alllogs: Recupera la base de datos a la última transacción o confirmación y aplica todos los registros requeridos.
  - -Hasta fecha: Recupera la base de datos hasta la fecha y hora especificadas.

    Debe usar el formato year-month-date: Hour: Minute: Second (yyyy-mm-dd:hh:mm:ss). Para horas, utilice el formato de 12 o 24 horas, según la configuración de la base de datos.

  - -Until scn: Permite avanzar los archivos de datos hasta alcanzar el número de cambio de sistema (SCN) especificado.
  - -Using-backup-Controlfile: Recupera la base de datos utilizando el archivo de control de copia de seguridad.
- **-restaurespec**

  Permite restaurar los datos en un sistema de archivos activo y restaurar desde los datos especificados mediante la asignación de cada copia Snapshot original a su sistema de archivos activo. Si no especifica una opción, SnapManager restaura los datos desde las copias Snapshot en el almacenamiento principal. Es posible especificar una de las siguientes opciones:

  - -Restoreespec: Especifica los datos que se van a restaurar y el formato de restauración.
- **-preview**

  Muestra la siguiente información:

  - Qué mecanismo de restauración (restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copia de archivos del lado del host) se utilizará para restaurar cada archivo
  - Por qué no se han utilizado mecanismos más eficientes para restaurar cada archivo, al especificar la opción -verbose Si está utilizando la opción -preview , debe saber lo siguiente:
  - La opción -force no afecta al comando.
  - La opción -recover no afecta al comando. Para obtener una vista previa de la operación de restauración, se debe montar la base de datos. Si desea obtener la vista previa de un plan de restauración y la base de datos no está montada actualmente, SnapManager monta la base de datos. Si no se puede montar la base de datos, el comando fallará y SnapManager devolverá la base de datos a su estado original.

  La opción -preview muestra hasta 20 archivos. Puede configurar el número máximo de archivos que se mostrará en el archivo smo.config.

- **-recover-from-location**

  Especifica la ubicación del registro de archivos externo de los archivos de registro de archivos.

SnapManager toma los archivos de registro de archivos de la ubicación externa y los utiliza para el proceso de recuperación.

- **-taskspec**

  Especifica el archivo XML de especificación de la tarea para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de restauración. Debe proporcionar la ruta de acceso completa del archivo XML de especificación de la tarea.

- **-dump**

  Especifica recoger los archivos de volcado después de la operación de restauración.

- **-fuerza**

  Si es necesario, cambia el estado de la base de datos a uno más bajo que el estado actual.

  De forma predeterminada, SnapManager puede cambiar el estado de la base de datos a más alto durante una operación. Esta opción no es necesaria para que SnapManager cambie el estado de la base de datos a uno más alto.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola. Puede usar esta opción para ver por qué no se pueden usar procesos de restauración más eficientes para restaurar el archivo.

Ejemplo

En el siguiente ejemplo se restaura una base de datos junto con los archivos de control:

```
smo backup restore -profile SALES1 -label full_backup_sales_May
-complete -controlfiles -force
```

Información relacionada

Restaurar backups de base de datos

Restaurar backups desde una ubicación alternativa

Creando especificaciones de restauración

El comando smo backup show

Puede usar el comando backup show para ver información detallada sobre un backup, incluido el estado de la protección, la clase de retención de backup y los backups en el almacenamiento principal y secundario.

Sintaxis

```
        smo backup show
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que se mostrarán las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- * etiqueta*

  Especifica la etiqueta del backup.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-id**

  Especifica el ID del backup.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos de la consola, al igual que cualquier información de clonación y verificación.

Ejemplo

El siguiente ejemplo muestra información detallada sobre el backup:

```
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
...
```

Información relacionada

Ver los detalles de backup

El comando de desmontaje del backup de smo

Puede ejecutar el comando backup umount para desmontar un backup.

Sintaxis

```
        smo backup unmount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea desmontar un backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id**

  Desmonta el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Desmonta el backup con la etiqueta especificada.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-dump**

  Recoge los archivos de volcado después de una operación de desmontaje correcta o con errores.

- **-fuerza**

  Desmonta el backup incluso si hay problemas en la liberación de los recursos asociados con el backup. SnapManager intenta desmontar el backup y borrar todos los recursos asociados. El registro muestra la operación de desmontaje correcta, pero es posible que deba limpiar los recursos de forma manual si hay errores en el registro.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

A continuación se muestra un ejemplo de una operación de desmontaje:

```
# 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
```

Información relacionada

Desmontaje de backups

El comando de actualización de backup de smo

Puede ejecutar el comando backup update para actualizar la política de retención de backups.

Sintaxis

```
        smo backup update
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-comment comment_text\]
[-quiet | -verbose]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que se actualizarán las copias de seguridad. El perfil contiene el identificador de

la base de datos y otra información de la base de datos.

- **-id guid**

  Verifica el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- * etiqueta*

  Especifica la etiqueta de backup y el alcance del backup como archivo de datos o registro de archivos.

- **-data**

  Especifica los archivos de datos.

- **-archivelogs**

  Especifica los archivos de registro de archivos.

- **-comment_text**

  Introduzca texto (hasta 200 caracteres) acerca de la actualización de copia de seguridad. Puede incluir espacios.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

- **-retener {-hora | -diario | -semanal | -mensual | -ilimitado}**

  Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si no se especifica -retain, la clase de retención predeterminada es -Hourly. Para retener las copias de seguridad para siempre, utilice la opción -Unlimited. La opción -Unlimited hace que la copia de seguridad no sea elegible para su eliminación.

Ejemplo

En el ejemplo siguiente se actualiza el backup para establecer la política de retención en Unlimited:

```
smo backup update -profile SALES1 -label full_backup_sales_May
-retain -unlimited -comment save_forever_monthly_backup
```

Información relacionada

Cambiar la política de retención de backups

Retención permanente de backups

El comando smo backup verify

Es posible ejecutar el comando backup verify para ver si el backup está en un formato válido para Oracle.

Sintaxis

```
        smo backup verify
-profile profile_name
[-label backup_name \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea verificar un backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Verifica el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando smo backup list para mostrar el GUID de cada backup.

- **-label label_name**

  Verifica el backup con la etiqueta especificada.

- **-dump**

  Recopila los archivos de volcado después de la operación de verificación de backup realizada correctamente o con errores.

- **-fuerza**

  Fuerza a la base de datos al estado necesario para realizar la operación de verificación.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

A continuación se muestra un ejemplo de verificación del backup:

```
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
```

Información relacionada

Verificación de los backups de las bases de datos

El comando smo clone create

Es posible ejecutar el comando clone create para crear el clon de una base de datos incluida en el backup. Es posible clonar un backup del almacenamiento primario o secundario.

Sintaxis

```
        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 \[, path2\]\]\[-taskspec
taskspec\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-nombre del perfil**

  Especifica la base de datos que desea clonar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-backup-id guid**

  Clona el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando list-verbose de backups de smo para mostrar el GUID de cada backup.

- **-backup-label backup_label_name**

  Especifica que se clone el backup con el nombre de etiqueta especificado.

- **-corriente**

  Especifica la creación de backup y clonado a partir del estado actual de la base de datos.

  > Si la base de datos se encuentra en el modo noarchivelog, SnapManager creará un backup sin conexión.

- **-newsid new_sid**

  Especifica un nuevo identificador exclusivo del sistema de Oracle para la base de datos clonada. El valor identificador del sistema es un máximo de ocho caracteres. Oracle no permite la ejecución simultánea de dos bases de datos con el mismo identificador de sistema en el mismo host.

- **-host target_host**

  Especifica el host en el que se debe crear el clon.

- **-label clone_label**

  Especifica una etiqueta para el clon.

- **-cadena de comentario**

  Especifica un comentario opcional para describir este clon. La cadena debe escribirse entre comillas simples.

  > Algunos vaciados eliminan las comillas. Si esto es cierto para el shell, debe escapar de las comillas con una barra invertida (\). Por ejemplo, es posible que tenga que introducir: \' esto es un comentario\'

- **-clonespec full_path_to_clonespec_file**

  Especifica la ruta de acceso al archivo XML de especificación del clon. Puede ser un nombre de ruta relativo o absoluto.

- **-syspassaword syspassaword**

  Especifica la contraseña para el usuario con privilegios sys.

  > Debe proporcionar la contraseña para el usuario con privilegios sys si las credenciales de la base de datos proporcionadas no son las mismas para el usuario con privilegios sys.

- **-reserva**

  Si se configura la opción -reserve en yes, se garantiza que la reserva de espacio garantizado para los

volúmenes nuevos. Si se configura la opción -reserve en no, se garantiza que la reserva de espacio garantizado de volumen se desactive para los volúmenes clones nuevos. Si se establece la opción -reserve en heredar, se garantiza que el nuevo clon herede las características de reserva de espacio de la copia Snapshot primaria. El valor predeterminado es no

En la siguiente tabla se describen los métodos de clonado y su efecto en la operación clone create y su opción -reserve. Una LUN se puede clonar mediante cualquiera de estos métodos.

Método de clonación	Descripción	Resultado
`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**

  Especifica omitir la recuperación de la base de datos, ejecutar la utilidad DBNEWID y no abrir la base de datos con los registros de nuevo mientras se crea el clon.

- **-recover-from-location**

  Especifica la ubicación del registro de archivos externo de los backups de registros de archivos donde SnapManager toma los archivos de registro de archivos de la ubicación externa y los utiliza para la clonado.

- **-taskspec**

  Especifica el archivo XML de especificación de la tarea para la actividad de procesamiento previo o la actividad de procesamiento posterior de la operación de clonado. Debe proporcionar la ruta de acceso completa del archivo XML de especificación de la tarea.

- **-dump**

  Especifica recoger los archivos de volcado después de la operación de creación de clones.

- **-silencio**

  Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se clona el backup mediante una especificación de clon que se crea para este clon:

```
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.
```

Información relacionada

Creando especificaciones de clon

Clonar bases de datos a partir de backups

El comando smo clone delete

Puede ejecutar el comando clone delete para eliminar un clon. No es posible eliminar un clon si utiliza algún operación.

Sintaxis

```
        smo clone delete
-profile profile_name
\[-id guid \| -label clone_name\]
[-login
\[-username db_username -password db_password -port db_port\]
 ]
\[-syspassword syspassword\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

Especifica el nombre del perfil que contiene el clon que se va a eliminar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-fuerza**

  Elimina el clon incluso si hay recursos asociados con el clon.

- **-id guid**

  Especifica el GUID del clon que se va a eliminar. SnapManager genera el GUID cuando se crea un clon. Puede usar el comando smo clone list para mostrar el GUID de cada clon.

- **-nombre de etiqueta**

  Especifica la etiqueta del clon que se va a eliminar.

- **-syspassaword syspassaword**

  Especifica la contraseña para el usuario con privilegios sys.

  > Debe proporcionar la contraseña para el usuario con privilegios sys si las credenciales de la base de datos proporcionadas no son las mismas para el usuario con privilegios sys.

- **-login**

  Permite introducir los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos.

- **-puerto db_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que describe el perfil.

- **-dump**

  Especifica que se recopilen los archivos de volcado después de la operación de eliminación de clones.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se elimina el clon:

```
smo clone delete -profile SALES1 -label SALES_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

El comando smo clone list

Este comando enumera los clones de la base de datos para un perfil determinado.

Sintaxis

```
        smo clone list
-profile profile_name
-delimiter character
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la lista de clones asociados con el perfil. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- * carácter delimitador*

  Cuando se especifica este parámetro, el comando enumera los atributos de cada fila separados por el carácter especificado.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se enumeran los clones de base de datos del perfil SALES1.

```
smo clone list -profile SALES1 -verbose
```

```
ID Status SID Host Label Comment
-------- ------- ----- ------- ---------- -------
8ab...01 SUCCESS hsdbc server1 back1clone test comment
```

Información relacionada

Ver una lista de clones

El comando smo clone show

Puede ejecutar el comando clone show para mostrar información sobre los clones de las bases de datos del perfil especificado.

Sintaxis

```
        smo clone show
-profile profile_name
\[-id  guid \| -label clone_name\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica la lista de clones asociados con el perfil. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id guid**

  Muestra información sobre el clon con el GUID especificado. SnapManager genera el GUID cuando se crea un clon. Puede usar el comando smo clone show para mostrar el GUID de cada clon.

- **-label label_name**

  Muestra información sobre el clon con la etiqueta especificada.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se muestra información sobre el clon:

```
smo clone show -profile SALES1 -label full_backup_sales_May -verbose
```

En la siguiente salida se muestra información sobre un clon de un backup en el almacenamiento primario:

```
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
```

Información relacionada

Visualización de información detallada de los clones

El comando de plantilla de clon de smo

Este comando permite crear una plantilla de especificación de clon.

Sintaxis

```
        smo clone template
-profile name
\[-backup-id guid  \| -backup-label backup_name\]
\[-quiet \| -verbose\]
```

Parámetros

- **-nombre del perfil**

Especifica la base de datos que desea crear una especificación de clon de. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-backup-id guid**

  Crea una especificación de clon a partir del backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Utilice el comando smo backup list para mostrar el GUID de cada backup.

- **-backup-label backup_label_name**

  Crea una especificación de clonado a partir del backup con la etiqueta de backup especificada.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo, se crea una plantilla de especificación de clon a partir del backup con la etiqueta full_backup_sales_May. Una vez completado el comando de plantilla de clon de smo, la plantilla de especificación del clon se completa.

```
smo clone template -profile SALES1 -backup-label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Información relacionada

Creando especificaciones de clon

Clonar bases de datos a partir de backups

El comando smo clone update

Este comando actualiza información acerca del clon. Puede actualizar el comentario.

Sintaxis

```
        smo clone update
-profile profile_name
\[-label label \| -id id\]
-comment  commment_text
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil que contiene el clon que desea actualizar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id**

  Especifica el ID del clon. SnapManager genera el ID cuando crea un clon. Use el comando smo clone list para mostrar el ID de cada clon.

- * etiqueta*

  Especifica la etiqueta del clon.

- **-comentario**

  Muestra el comentario introducido en la creación del clon. Este es un parámetro opcional.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se actualiza el comentario del clon.

```
smo clone update -profile anson.pcrac5
-label clone_pcrac51_20080820141624EDT -comment See updated clone
```

El comando smo clone detach

Después de dividir un volumen clonado de su volumen principal en Data ONTAP, se puede ejecutar el comando clone detach desde SnapManager para hacer saber a SnapManager que el volumen ya no es un clon.

Sintaxis

desacoplamiento del clon de smo -profile profile_name -label clone_label

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil a partir del cual se crea el clon.

- **-label clone_label**

  Especifica el nombre generado por la operación de clonado.

Ejemplo

El siguiente comando desvincula el clon:

```
smo clone detach -profile SALES1 -label sales1_clone
```

El comando cmdfile de smo

Puede utilizar el comando cmdfile para ejecutar cualquier comando si el shell del host limita el número de caracteres que pueden aparecer en una línea de comandos.

Sintaxis

```
        smo cmdfile
-file file_name
\[-quiet \| -verbose\]
```

Puede incluir el comando en un archivo de texto y usar el comando cmdfile de smo para ejecutar el comando. Sólo puede agregar un comando en un archivo de texto. No debe incluir smo en la sintaxis de comandos.

> El comando cmdfile de smo reemplaza al comando pfile de smo. El archivo cmdsmo no es compatible con el comando pfile de smo.

Parámetros

- **-file file_name**

  Especifica la ruta de acceso al archivo de texto que contiene el comando que desea ejecutar.

- **-silencio**

  Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

El comando smo credential clear

Este comando borra la caché de las credenciales de usuario de todos los recursos protegidos.

Sintaxis

```
        smo credential clear
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En este ejemplo se borran todas las credenciales del usuario que ejecuta el comando.

```
smo credential clear -verbose
```

```
SMO-20024 [INFO ]: Cleared credentials for user "user1".
```

Información relacionada

Borrar credenciales de usuario para todos los hosts, repositorios y perfiles

El comando smo credential delete

Este comando elimina las credenciales de usuario de un recurso protegido en particular.

Sintaxis

```
        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]
```

Parámetros

- **-host hostname**

  Especifica el nombre del servidor host en el que se ejecuta SnapManager.

  El parámetro -host incluye las siguientes opciones:

  - -Name host_name: Especifica el nombre del host para el que se eliminará la contraseña.
  - -Username user_name: Especifica el nombre de usuario en el host.
- **-repository -dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

  El parámetro -Repository incluye las siguientes opciones:

  - -Dbnamerepo_service_name: Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.
  - -Host repo_host: Especifica el nombre o la dirección IP del servidor host en el que se ejecuta la base de datos de repositorio.
  - -Login-username repo_username: Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.
  - -Port repo_Port: Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.
- **-profile -name profile_name**

  Especifica el perfil con el que está asociada la base de datos.

  El parámetro -profile incluye la siguiente opción:

  - -Name profilename: Especifica el nombre del perfil para el que se eliminará la contraseña.
- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En este ejemplo se eliminan las credenciales del perfil.

```
smo credential delete -profile -name user1 -verbose
```

```
SMO-20022 [INFO ]: Deleted credentials and repository mapping
 for profile "user1" in user credentials for "user1".
```

En este ejemplo, se eliminan las credenciales del repositorio.

```
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".
```

En este ejemplo, se eliminan las credenciales del host.

```
smo credential delete -host -name Host2
```

```
SMO-20033 [INFO ]: Deleted host credentials for "Host2" in user
credentials for "user1".
```

Información relacionada

Eliminación de credenciales para recursos individuales

El comando smo credential list

Este comando enumera todas las credenciales de un usuario.

Sintaxis

```
        smo credential list
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

Este ejemplo muestra todas las credenciales del usuario que ejecuta el comando.

```
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
```

Información relacionada

Visualización de las credenciales de usuario

El comando smo credential set

Este comando permite establecer las credenciales para que los usuarios accedan a recursos seguros, como hosts, repositorios y perfiles de bases de datos. La contraseña del host es la contraseña del usuario en el host donde se ejecuta SnapManager. La contraseña del repositorio es la contraseña del usuario de Oracle que contiene el esquema del repositorio de SnapManager. La contraseña del perfil es una contraseña compuesta por la persona que crea el perfil. Para las opciones de host y repositorio, si no se incluye la opción -password opcional, se le pedirá que introduzca una contraseña del tipo especificado en los argumentos de comando.

Sintaxis

```
        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 \|
\[-profile
-name profile_name\]
\[-password password\] \]
\[-quiet \| -verbose\]
```

Parámetros

- **-host hostname**

  Especifica el nombre o la dirección IP del servidor host en el que se ejecuta SnapManager.

  El parámetro -host incluye las siguientes opciones:

  - -Name host_name: Especifica el nombre del host para el que se establecerá la contraseña.
  - -Username user_name: Especifica el nombre de usuario en el host.
  - -Password password: Especifica la contraseña del usuario en el host.
- **-repository -dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

  El parámetro -Repository incluye las siguientes opciones:

  - -Dbnamerepo_service_name: Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.
  - -Host repo_host: Especifica el nombre o la dirección IP del servidor host en el que se ejecuta la base de datos de repositorio.
  - -Login-username repo_username: Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.
  - -Password password: Especifica la contraseña necesaria para acceder a la base de datos que almacena el repositorio.
  - -Port repo_Port: Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.
- **-profile -name profile_name**

  Especifica el perfil con el que está asociada la base de datos.

  El parámetro -profile incluye la siguiente opción:

- -Name profilename: Especifica el nombre del perfil para el que va a configurar la contraseña.
- -Password password: Especifica la contraseña necesaria para acceder al perfil.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando para configurar las credenciales del repositorio

En el ejemplo siguiente se establecen credenciales para un repositorio.

```
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.
```

Ejemplo de comando para configurar las credenciales del host

Dado que las credenciales de host representan una credencial real del sistema operativo, deben incluir el nombre de usuario además de la contraseña.

```
smo credential set -host -name bismarck -username avida
Password for avida@bismarck : ********
Confirm password for avida@bismarck : ********
```

Información relacionada

Cómo mantiene SnapManager la seguridad

El comando smo history list

Este comando le permite ver una lista de detalles del historial de la operación SnapManager.

Sintaxis

```
        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\}
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica la operación SnapManager para la que se configura el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history list -profile -name PROFILE1 -operation -operations
backup -verbose
```

El comando Operation-show de historial de smo

Este comando le permite ver el historial de una operación de SnapManager específica asociada con un perfil.

Sintaxis

```
        smo history operation-show
-profile profile
\{-label label \| -id id\}
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- * etiqueta | -idid*

  Especifica el ID o la etiqueta de la operación de SnapManager para la que desea ver el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history operation-show -profile PROFILE1 -label backup1
-verbose
```

El comando smo history purge

Este comando le permite eliminar el historial de operaciones de SnapManager.

Sintaxis

```
        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\}
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica la operación SnapManager para la que se configura el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

El comando smo history remove

Este comando permite quitar el historial de operaciones de SnapManager asociadas con un único perfil, varios perfiles o todos los perfiles bajo un repositorio.

Sintaxis

```
        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\}
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

  Especifica la operación SnapManager para la que se configura el historial.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

El comando smo history set

Puede ejecutar el comando History Set para configurar las operaciones para las que desea ver el historial.

Sintaxis

```
        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]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. El nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repositorio**

  Especifica los detalles de la base de datos que almacena el perfil.

- **-dbname repo_dbname**

  Especifica el nombre de la base de datos que almacena el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del host donde reside la base de datos del repositorio.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto del Protocolo de control de transmisión (TCP) que se utiliza para acceder a la base de datos del repositorio.

- **-operation {-operationsoperation_name [operation_name1, operation_name2] | -all**

Especifica las operaciones de SnapManager para las que se desea configurar el historial.

- **-retenga {-countretain_count | -dailydaily_count | -mensual-mensual_count | -weeklyweekly_count}**

  Especifica la clase de retención de las operaciones de creación de backup, verificación de backup, restauración y recuperación, y creación de operaciones de clonado. La clase de retención se establece en función del número de recuento de operaciones, el número de días, semanas o meses.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

El siguiente ejemplo muestra información sobre la operación de backup:

```
smo history set -profile -name PROFILE1 -operation -operations backup
-retain -daily 6
 -verbose
```

El comando smo history show

Este comando le permite ver información detallada del historial de un perfil en concreto.

Sintaxis

```
        smo history show
-profile profile
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

```
          smo  history show -profile -name PROFILE1
 -verbose
```

El comando smo help

Puede ejecutar el comando help para mostrar información acerca de los comandos de la SnapManager y sus opciones. Si no proporciona un nombre de comando, se muestra una lista de comandos válidos. Si proporciona un nombre de comando, muestra la sintaxis de ese comando.

Sintaxis

```
        smo help
\[\]\[backup\|cmdfile\|clone\|credential\|help\|operation\|profile\|reposi
tory\|system\|version\|plugin\|diag\|history\|schedule\|notification\|stor
age\|get\]
\[-quiet \| -verbose\]
```

Parámetros

A continuación se muestran algunos nombres de comandos que puede utilizar con este comando:

- Backup
- clonar
- cmdfile
- credencial
- diag
- obtenga
- notificación
- ayuda
- historia
- funcionamiento
- plug-in
- perfil
- repositorio
- programación
- Reducida
- sistema
- versión

El comando remove-summary-notification de la notificación de smo

Este comando deshabilita la notificación de resumen de varios perfiles en una base de datos de repositorio.

Sintaxis

```
        smo notification remove-summary-notification
-repository
-dbname repo_service_name
-port repo_port
-host repo_host
-login -username repo_username
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login repo_username**

  Especifica el nombre de inicio de sesión necesario para acceder a la base de datos que almacena el repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

En el siguiente ejemplo se deshabilita la notificación de resumen de varios perfiles en una base de datos de repositorio.

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login -username oba5
```

El comando de notificación de actualización-resumen-notificación de smo

Puede ejecutar el comando notification update-summary-notification para habilitar la notificación de resumen para una base de datos de repositorio.

Sintaxis

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Especifica los detalles de la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos del repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos del repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del host en el que reside la base de datos del repositorio.

- **-login**

Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-email-dirección1,e-mail-dirección2**

  Especifica las direcciones de correo electrónico de los destinatarios.

- **-tema-patrón**

  Especifica el patrón del asunto del correo electrónico.

- **-frequency { -daily --time daily_time | -time --time_time | -quannual --time mensual_time -date {1|2|3…|31 } | -semanal --time weekly_time -day {1|2|3|4|5|6|7 }**

  Especifica el tipo de programación y la hora de la programación en el momento en que desea recibir la notificación por correo electrónico.

- **-profile1, profile2**

  Especifica los nombres de perfil que requieren notificación por correo electrónico.

- **-notification-host-notification-host**

  Especifica el host del servidor SnapManager desde el cual se envía el correo electrónico de notificación de resumen a los destinatarios. Puede proporcionar un nombre de host o una dirección IP para el host de notificación. También es posible actualizar la dirección IP del host o el nombre de host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se habilita la notificación de resumen para una base de datos de repositorio:

```
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
```

El comando smo notification set

Puede utilizar el comando Notification Set para configurar el servidor de correo.

Sintaxis

```
        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]
```

Parámetros

- **-sender-email email_address**

  Especifica la dirección de correo electrónico del remitente desde la cual se envían las alertas por correo electrónico. En SnapManager 3.2 para Oracle, puede incluir un guión (-) al especificar el nombre de dominio de la dirección de correo electrónico. Por ejemplo, puede especificar la dirección de correo electrónico del remitente como -sender-email07lbfmdatacenter@continental-corporation.com.

- **-mailhost**

  Especifica el nombre o la dirección IP del servidor host que gestiona las notificaciones por correo electrónico.

- **-mailport**

  Especifica el número de puerto del servidor de correo.

- **-authentication -username -password**

  Especifica los detalles de autenticación de la dirección de correo electrónico. Debe especificar el nombre de usuario y la contraseña.

- **-repositorio**

  Especifica los detalles de la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto del Protocolo de control de transmisión (TCP) que se utiliza para acceder a la base de datos del repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos del repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host repo_host**

  Especifica el nombre o la dirección IP del host donde reside la base de datos del repositorio.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo, se configura el servidor de correo:

```
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
```

El comando de volcado de la operación de smo

Puede ejecutar el comando operation dump para crear un archivo JAR que contenga información de diagnóstico acerca de una operación.

Sintaxis

```
        smo operation dump
-profile profile_name
\[-label label_name \| -id guid\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea crear los archivos de volcado. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-label label_name**

  Crea archivos de volcado para la operación y asigna la etiqueta especificada.

- **-id guid**

  Crea archivos de volcado para la operación con el GUID especificado. SnapManager genera el GUID cuando se inicia la operación.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se crea el archivo de volcado para la copia de seguridad:

```
smo operation dump -profile SALES1
-id 8abc01ec0e78f3e2010e78f3fdd00001
```

```
Dump file created Path:
C:\userhomedirectory\netapp\smo\3.3\smo_dump_8abc01ec0e78f3e2010e78f3fdd00
001.jar
```

Información relacionada

Volcar archivos

El comando smo operation list

Este comando muestra la información resumida de todas las operaciones registradas en un perfil especificado.

Sintaxis

```
        smo operation list
-profile profile_name
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- * carácter delimitador*

  (Opcional) cuando se especifica este parámetro, el comando enumera cada fila en una línea independiente y los atributos de esa fila están separados por el carácter especificado.

- **-silencio**

  (Opcional) sólo muestra mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  (Opcional) muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo, se muestra la información de resumen de todas las operaciones registradas con el perfil especificado.

```
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
```

Información relacionada

Ver una lista de operaciones

El comando smo operation show

Puede ejecutar el comando operation show para mostrar la información de resumen de todas las operaciones realizadas en el perfil especificado. La salida muestra el usuario cliente (el usuario del PC cliente) y el usuario efectivo (el usuario de SnapManager que es válido en el host seleccionado).

Sintaxis

```
        smo operation show
-profile profile_name
\[-label label \| -id id\]
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- * etiqueta*

  Especifica la etiqueta de la operación.

- **-id**

  Especifica el identificador de la operación.

- **-silencio**

  Opcional: Muestra solo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Opcional: Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

La siguiente línea de comandos muestra información detallada sobre una operación:

```
# 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
```

Información relacionada

Ver los detalles de la operación

El comando smo password reset

Puede ejecutar el comando de restablecimiento de contraseña para restablecer la contraseña de un perfil.

Sintaxis

```
        smo password reset
-profile profile
\[-profile-password profile_password\]
\[-repository-hostadmin-password repository_hostadmin_password\]
[-quiet | -verbose]
```

Parámetros

- * perfil*

Especifica el nombre del perfil para el que desea restablecer la contraseña.

- **-profile-password profile_password**

  Especifica la nueva contraseña para el perfil.

- **-repository-hostadmin-password admin_password**

  Especifica la credencial de usuario autorizado con privilegios de administrador local para la base de datos del repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo profile create

Puede ejecutar el comando profile create para crear un perfil de una base de datos en un repositorio. Debe montar la base de datos antes de ejecutar este comando.

Sintaxis

```
        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]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-profile-password profile_password**

  Especifique la contraseña del perfil.

- **-repositorio**

  Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-sid db_sid**

Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo con la opción -sid.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos del repositorio.

- **-base de datos**

  Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host db_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-login**

  Especifica los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-puerto db_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que describe el perfil.

- **-rman**

  Especifica los detalles que utiliza SnapManager para catalogar los backups con Oracle Recovery Manager (RMAN).

- **-controllfile**

  Especifica los archivos de control de la base de datos de destino en lugar de un catálogo como repositorio de RMAN.

- **-login**

  Especifica los detalles de inicio de sesión de RMAN.

- **-password rman_password**

  Especifica la contraseña que se utiliza para iniciar sesión en el catálogo de RMAN.

- **-username rman_username**

  Especifica el nombre de usuario utilizado para iniciar sesión en el catálogo de RMAN.

- **-tnsname tnsname**

  Especifica el nombre de conexión tnsname (que se define en el archivo tsname.ora).

- **-retener [-recuento n] [-duración m]] [-número n] [-duración m]] [-número n] [-duración m] [-número n] [-duración m]] [-mensual [-recuento n] [-duración m]]**

  Especifica la política de retención para un backup donde se cuenta un número de retención o ambos, junto con una duración de retención para una clase de retención (por hora, día, semana, mes).

  Para cada clase de retención, se puede especificar un recuento de retención o una duración de retención. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). Por ejemplo, si el usuario especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-comentario**

  Especifica el comentario de un perfil que describe el dominio del perfil.

- **-snapname-pattern patrón**

  Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han creado. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-resumen-notificación**

  Especifica que la notificación de resumen por correo electrónico está activada para el nuevo perfil.

- **-notification -success-email-mail_dirección1,dirección de correo electrónico.2 -subject_pattern**

  Especifica que la notificación de correo electrónico está habilitada para el nuevo perfil de forma que los destinatarios reciban correos electrónicos cuando la operación de SnapManager se realice correctamente. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del nuevo perfil.

  También se puede incluir texto de asunto personalizado para el nuevo perfil. Puede cambiar el texto del asunto cuando cree un perfil o después de que se haya creado el perfil. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-notification -failure -email correo-e_dirección1,dirección de correo-e-dirección2 -subject_pattern**

  Especifica que la habilitación de la notificación por correo electrónico está habilitada para el nuevo perfil, de modo que los destinatarios reciban los correos electrónicos cuando falle la operación de SnapManager. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del nuevo perfil.

  También se puede incluir texto de asunto personalizado para el nuevo perfil. Puede cambiar el texto del asunto cuando cree un perfil o después de que se haya creado el perfil. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-separate-archivvelog-backups**

  Especifica que el backup de registros de archivos está separado del backup del archivo de datos. Este es un parámetro opcional que puede proporcionar al crear el perfil. Después de separar el backup con esta opción, es posible tomar el backup solo de los archivos de datos o el backup de solo los registros de archivos.

- **-retain-archivvelog-backups -horas | -daysdays | -weeksweeks| -months**

  Especifica que los backups de los registros de archivos se retendrán según la duración de la retención del registro de archivos (hora, día, semana, mensual).

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

- **-include-with-online-backups**

  Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

- **-no-include-with-online-backups**

  Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

  Especifica que los archivos de volcado se recopilan después de la operación de creación de perfiles correcta.

Ejemplo

El siguiente ejemplo muestra la creación de un perfil con una política de retención de horas y notificaciones por correo electrónico:

```
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.
```

Información relacionada

Gestionar perfiles para backups eficientes

Nomenclatura de copias Snapshot

Cómo SnapManager retiene los backups en el almacenamiento local

El comando smo profile delete

Puede ejecutar el comando profile delete para eliminar un perfil de la base de datos.

Sintaxis

```
        smo profile delete
-profile profile
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el perfil que se va a eliminar.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se elimina el perfil:

```
smo profile delete -profile SALES1
Operation Id [Ncaf00af0242b3e8dba5c68a57a5ae932] succeeded.
```

Información relacionada

Eliminar perfiles

El comando smo profile dump

Puede ejecutar el comando profile dump para crear el archivo .jar que contiene información de diagnóstico acerca de un perfil.

Sintaxis

```
        smo profile dump
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el perfil para el que desea crear los archivos de volcado. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se crea un volcado para el perfil SALES1:

```
smo profile dump -profile SALES1
Dump file created
Path:
C:\\userhomedirectory\\netapp\\smo\\3.3.0\\smo_dump_SALES1_hostname.jar
```

El comando smo profile list

Este comando muestra una lista de los perfiles actuales.

Sintaxis

```
        smo profile list
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se muestran los perfiles existentes con sus detalles.

```
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: ********
```

El comando smo profile show

Puede ejecutar el comando profile show para mostrar la información de un perfil.

Sintaxis

```
        smo profile show
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo profile SYNC

Este comando carga las asignaciones de perfil a repositorio para ese repositorio en un archivo del directorio inicial en el host local.

Sintaxis

```
        smo profile sync
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login
-username repo_username
                \[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica la base de datos del repositorio para el perfil que se va a sincronizar.

- **-host**

  Especifica el host de la base de datos.

- **-puerto**

  Especifica el puerto para el host.

- **-login**

  Especifica el proceso de inicio de sesión para el usuario host.

- **-nombre de usuario**

  Especifica el nombre de usuario para el host.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el siguiente ejemplo se muestra el resultado del comando para sincronizar las asignaciones de perfil a repositorio de la base de datos.

```
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.
```

El comando smo profile update

Puede ejecutar el comando profile update para actualizar la información de un perfil existente.

Sintaxis

```
        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]
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-profile-password profile_password**

  Especifica la contraseña del perfil.

- **-new-profile new_profile_name**

  Especifica el nuevo nombre que puede proporcionar para un perfil.

- **-base de datos**

  Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos de la que se realizará un backup, se restaurará, etc.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-sid db_sid**

  Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo mediante la opción -sid.

- **-login**

  Especifica los detalles de inicio de sesión del repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP necesario para acceder a la base de datos del repositorio.

- **-base de datos**

  Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname db_dbname**

  Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host db_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-login**

  Especifica los detalles de inicio de sesión de la base de datos.

- **-username db_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password db_password**

  Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-puerto db_port**

  Especifica el número de puerto TCP necesario para acceder a la base de datos que describe el perfil.

- **-rman**

  Especifica los detalles que utiliza SnapManager para catalogar los backups con Oracle Recovery Manager (RMAN).

- **-controllfile**

  Especifica los archivos de control de la base de datos de destino en lugar de un catálogo como repositorio de RMAN.

- **-login**

  Especifica los detalles de inicio de sesión de RMAN.

- **-password rman_password**

  Especifica la contraseña que se utiliza para iniciar sesión en el catálogo de RMAN.

- **-username rman_username**

  Especifica el nombre de usuario utilizado para iniciar sesión en el catálogo de RMAN.

- **-tnsname tnsname**

  Especifica el nombre de conexión tnsname (que se define en el archivo tsname.ora).

- **-remove-rman**

  Especifica la eliminación de RMAN en el perfil.

- **-retener [-contador hora [-compensn] [-duración m]] [-diario [-conteo n] [-duración m] [-semanal [-conteo n][-duración m]] [-mensual [-conteo n][-duración m]]**

  Especifica la clase de retención (por hora, por día, por semana o por mes) para una copia de seguridad.

  Para cada clase de retención, se puede especificar un recuento de retención, una duración de retención o

ambas. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora o días por día). Por ejemplo, si el usuario especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-comentario**

  Especifica el comentario de un perfil.

- **-snapname-pattern patrón**

  Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han producido. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-resumen-notificación**

  Especifica que la notificación de resumen por correo electrónico está activada para el perfil existente.

- **-notificación [-success-email e-mail_dirección1,dirección de e-mail.2 -subject_pattern]**

  Habilita la notificación de correo electrónico para el perfil existente de forma que los destinatarios reciban los correos electrónicos cuando la operación SnapManager se realice correctamente. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del correo electrónico para el perfil existente.

  Puede cambiar el texto del asunto al actualizar el perfil o incluir texto de asunto personalizado. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-notificación [-failure -email e-mail_dirección1,dirección de e-mail.2 -subject_pattern]**

  Habilita la notificación de correo electrónico para el perfil existente de modo que los destinatarios reciban los correos electrónicos cuando falle la operación de SnapManager. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del correo electrónico para el perfil existente.

  Puede cambiar el texto del asunto al actualizar el perfil o incluir texto de asunto personalizado. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-separate-archivvelog-backups**

  Separa el backup de registros de archivos del backup de archivo de datos. Este es un parámetro opcional que puede proporcionar al crear el perfil. Después de separar los backups se separan con esta opción, es posible crear un backup de solo los archivos de datos o un backup de solo los registros de archivos.

- **-retain-archivvelog-backups -horas | -daysdays | -weeksweeks| -months**

  Especifica que los backups de los registros de archivos se retendrán según la duración de la retención del registro de archivos (hora, día, semana, mensual).

- **-include-with-online-backups | -no-include-with-online-backups**

  Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

  Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

  Especifica que los archivos de volcado se recopilan después de la operación de creación de perfiles correcta.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se cambia la información de inicio de sesión de la base de datos descrita por el perfil y se configura la notificación por correo electrónico para este perfil:

```
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.
```

Información relacionada

Cambio de contraseñas de perfil

Cómo SnapManager retiene los backups en el almacenamiento local

El comando smo profile verify

Puede ejecutar el comando profile verify para verificar la configuración del perfil. Debe montar la base de datos antes de ejecutar este comando.

Sintaxis

```
        smo profile verify
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-perfil**

  Especifica el perfil que se va a verificar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el siguiente ejemplo se verifica el perfil:

```
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.
```

Información relacionada

Verificando perfiles

El comando smo repository create

Sintaxis

Este comando crea un repositorio en el que se almacenan perfiles de base de datos y credenciales asociadas. Este comando también comprueba si el tamaño de los bloques es adecuado.

```
        smo repository create
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Se intenta forzar la creación del repositorio. Con esta opción, SnapManager se solicita que se realice un backup del repositorio antes de crear el repositorio.

- **-noprompt**

  No muestra el símbolo del sistema de realizar una copia de seguridad del repositorio antes de crearlo si utiliza la opción -force. El uso de la opción -noprompt garantiza que el prompt no aparezca, facilitando la creación de repositorios con un script.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando

El siguiente ejemplo crea un repositorio en la base de datos SMOREPO en el hotspur del host.

```
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
```

Información relacionada

Creación de repositorios

El comando smo repository delete

Este comando elimina un repositorio utilizado para almacenar perfiles de base de datos y credenciales asociadas. Sólo puede eliminar un repositorio si no hay perfiles en el repositorio.

Sintaxis

```
        smo repository delete
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Se intenta forzar la eliminación del repositorio, incluso si hay operaciones incompletas. SnapManager emite un aviso si existen operaciones incompletas, en las que se pregunta si está seguro de que se desea eliminar el repositorio.

- **-noprompt**

  No se le solicita antes de eliminar el repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la eliminación de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando

En el ejemplo siguiente se elimina el repositorio de la base de datos SALESDB.

```
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".
```

El comando rollback del almacén de smo

Este comando permite revertir o revertir una versión superior de SnapManager a la versión original de la que se actualizó.

Sintaxis

```
        smo repository rollback
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-rollbackhost host_with_target_database
[-force]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-rollbackhost host host_with_target_database**

  Especifica el nombre del host que se va a revertir de una versión superior de SnapManager a la versión anterior original.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

  No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smo repository rollback -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -rollbackhost hostA
```

El comando rollingupgrade del almacén de smo

Este comando realiza la actualización en un solo host o de varios hosts y las bases de datos de destino asociadas desde una versión inferior de SnapManager a una versión

posterior. El host actualizado solo se gestiona con la versión superior de SnapManager.

Sintaxis

```
        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]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-actualizehost host_with_target_database**

  Especifica el nombre del host que se actualizará de una versión inferior de SnapManager a una versión superior.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

  No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smo repository rollingupgrade -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -upgradehost hostA
```

El comando smo repository show

Este comando muestra información sobre el repositorio.

Sintaxis

```
        smo repository show
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del

repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo de comando

En el siguiente ejemplo se muestran detalles sobre el repositorio de la base de datos SALESDB.

```
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
```

El comando de actualización del almacén de smo

Este comando actualiza el repositorio que almacena perfiles de base de datos y las credenciales asociadas al actualizar SnapManager. Cada vez que instale una nueva versión de SnapManager, debe ejecutar el comando de actualización del repositorio para

poder utilizar la nueva versión. Puede utilizar este comando solo si no hay comandos incompletos en el repositorio.

Sintaxis

```
        smo repository update
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parámetros

- **-repositorio**

  Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname repo_service_name**

  Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host repo_host**

  Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

  Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo_username**

  Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo_port**

  Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-fuerza**

  Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

  No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción -noprompt garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521
```

El comando smo schedule create

Es posible utilizar el comando schedule create para programar la creación de un backup en un momento específico.

Sintaxis

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos para la que desea programar el backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-opción automática**

  Si la base de datos está en estado montado o sin conexión, SnapManager realiza un backup sin conexión. Si la base de datos está en estado abierto o en línea, SnapManager realiza un backup en línea. Si se utiliza la opción -force con la opción -offline, SnapManager fuerza un backup sin conexión aunque la base de datos esté actualmente en línea.

- **-opción en línea**

  Especifica un backup de base de datos en línea.

- **-opción sin conexión**

Especifica un backup sin conexión mientras la base de datos está en estado de apagado. Si la base de datos está en estado abierto o montado, el backup genera errores. Si se utiliza la opción -force, SnapManager intenta modificar el estado de la base de datos para cerrar la base de datos con el fin de realizar una copia de seguridad sin conexión.

- **-opción completa**

  Realiza un backup de toda la base de datos. Esto incluye todos los datos, registros archivados y archivos de control. Se realiza una copia de seguridad de los redo logs archivados y de los archivos de control, independientemente del tipo de copia de seguridad que realice. Si se desea realizar un backup solo de una parte de la base de datos, se deben utilizar la opción -files o -tablespaces.

- **-lista de archivos**

  Realiza un backup solo de los archivos de datos especificados, además de los archivos de registro y control archivados. Separe la lista de nombres de archivo con espacios. Si la base de datos está en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-tablespaces**

  Realiza un backup solo de los espacios de tablas de la base de datos especificados, además de los archivos de registro y control archivados. Separe los nombres de tablespace con espacios. Si la base de datos está en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-nombre de etiqueta**

  Especifica un nombre opcional para este backup. Este nombre debe ser único dentro del perfil. El nombre puede contener letras, números, guiones bajos (_) y guiones (-). No puede comenzar con un guión.

  Si no se especifica una etiqueta, SnapManager crea una etiqueta predeterminada en el formato scope_type_date:

  - El ámbito es F indicar un backup completo o P para indicar un backup parcial.
  - El tipo es C para indicar una copia de seguridad sin conexión (en frío), H para indicar una copia de seguridad en línea (activa) o A para indicar una copia de seguridad automática, por ejemplo, P_A_20081010060037IST.
  - Fecha es el año, el mes, el día y la hora de la copia de seguridad.

    SnapManager se usa un reloj de 24 horas.

  Por ejemplo, si realizó un backup completo con la base de datos sin conexión el 16 de enero de 2007, a las 5:45:16 Hora estándar del este, SnapManager crearía la etiqueta F_C_20070116174516EST.

- **-cadena de comentario**

  Especifica un comentario opcional para describir esta copia de seguridad. La cadena debe escribirse entre comillas simples (').

  > Algunos vaciados pelan entre comillas. Si esto es cierto para el shell, debe incluir la comillas con una barra diagonal inversa (\). Por ejemplo, es posible que deba introducir: `\' this is a comment\'`.

- **-verificar opción**

  Verifica que los archivos de la copia de seguridad no están dañados ejecutando la utilidad oracle dbv.

  > Si se especifica la opción -Verify, la operación de backup no se completará hasta que finalice la operación de verificación.

- **-opción de fuerza**

  Fuerza un cambio de estado si la base de datos no está en el estado correcto. Por ejemplo, SnapManager puede cambiar el estado de la base de datos de en línea a sin conexión, según el tipo de backup especificado y el estado en el que está la base de datos.

  - Si la instancia local está en estado de apagado y al menos una instancia está abierta, puede cambiar la instancia local a montada mediante la opción -force .
  - Si no hay ninguna instancia abierta, puede cambiar la instancia local a abierta mediante la opción -force.

- **-retener { -hora | -diario | -semanal | -mensual | -ilimitado}**

  Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si no se especifica la opción -retain, la clase de retención predeterminada es -Hourly. Para retener las copias de seguridad para siempre, utilice la opción -Unlimited. La opción -Unlimited hace que el backup no sea apto para que lo elimine la política de retención.

- **-archivelogs**

  Especifica la creación de un backup de registro de archivos.

- **-backup-más extraño path1, [, [path2]]**

  Especifica los destinos de registros de archivos para el backup de registros de archivos.

- **-exclude-más extraño path1, [, [path2]]**

  Especifica los destinos de registro de archivos que se excluirán de la copia de seguridad.

- **-prunelogs {-all | -until-scnuntil-scn | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-meses | -días | -semanas | -horas}**

  Especifica si se eliminarán los archivos de registro de archivos de los destinos de registro de archivos en función de las opciones proporcionadas al crear un backup. La opción -all elimina todos los archivos de registro de archivos de los destinos de registro de archivos. La opción -until-scn elimina los archivos de registro de archivos hasta que se especifique un número de cambio de sistema (SCN). La opción -until -date elimina los archivos de registro de archivos hasta el periodo de tiempo especificado. La opción -before elimina los archivos de registro de archivos antes del periodo de tiempo especificado (días, meses, semanas, horas).

- **-nombre-horario nombre_horario**

  Especifica el nombre que se proporcionará para la programación.

- **-schedule-comentario schedule_comment**

  Especifica un comentario opcional que se va a describir acerca de la programación del backup.

- **-interval { -time | -daily | -semanal | -mensual | -onetimeonly}**

  Especifica el intervalo de tiempo mediante el cual se crean los backups. Se puede programar el backup cada hora, día, semana, mes o solo una vez.

- **-cronstring cron_string**

  Especifica la programación del backup mediante cronstring. Las expresiones cron se utilizan para configurar instancias de CronTrigger. Las expresiones cron son cadenas que se componen de las siguientes subexpresiones:

  - 1 se refiere a segundos.
  - 2 se refiere a minutos.
  - 3 se refiere a horas.
  - 4 se refiere a un día en un mes.
  - 5 se refiere al mes.
  - 6 se refiere a un día en una semana.
  - 7 se refiere al año (opcional).

- **-hora de inicio aaaa-MM-dd HH:mm**

  Especifica la hora de inicio de la operación programada. La hora de inicio de la programación debe incluirse en el formato aaaa-MM-dd HH:mm.

- **-runasuser runasuser**

  Especifica si se cambia el usuario (usuario raíz o usuario de Oracle) de la operación de backup programada mientras se programa el backup.

- **-tasktaskspec**

  Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. La ruta completa del archivo XML debe proporcionarse con la opción -taskspec .

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

El comando smo schedule delete

Este comando elimina una programación de backup cuando ya no es necesaria.

Sintaxis

```
        smo schedule delete
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea eliminar una programación de backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre de programación que se proporcionó al crear una programación de backups.

El comando smo schedule list

Este comando, enumera las operaciones programadas asociadas con un perfil.

Sintaxis

```
        smo schedule list
-profile profile_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos, mediante el cual puede ver una lista de operaciones programadas. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

El comando smo schedule resume

Este comando reanuda la programación de backup suspendida.

Sintaxis

```
        smo schedule resume
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea reanudar la programación de backups suspendida. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre de programación que se proporcionó al crear una programación de backups.

El comando smo schedule suspend

Este comando suspende una programación de backup hasta que se reanuda la programación de backup.

Sintaxis

```
        smo schedule suspend
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea suspender una programación de backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre de programación que se proporcionó al crear una programación de backups.

El comando smo schedule update

Este comando actualiza la programación de una copia de seguridad.

Sintaxis

```
        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
\[-quiet \| -verbose\]
```

Parámetros

- **-profile profile_name**

  Especifica el nombre del perfil relacionado con la base de datos que desea programar el backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-nombre-horario nombre_horario**

  Especifica el nombre que se proporcionará para la programación.

- **-schedule-comentario schedule_comment**

  Especifica un comentario opcional que se va a describir acerca de la programación del backup.

- **-interval { -time | -daily | -semanal | -mensual | -onetimeonly}**

  Indica el intervalo de tiempo mediante el cual se crean los backups. Se puede programar el backup cada hora, día, semana, mes o una sola vez.

- **-cronstring cron_string**

  Especifica la programación del backup mediante cronstring. Las expresiones cron se utilizan para configurar instancias de CronTrigger. Las expresiones cron son cadenas que se componen de siete subexpresiones:

  - 1 se refiere a segundos
  - 2 se refiere a minutos
  - 3 se refiere a horas
  - 4 se refiere a un día en un mes
  - 5 se refiere al mes
  - 6 se refiere a un día en una semana
  - 7 se refiere al año (opcional)

- **-hora de inicio aaaa-MM-dd HH:mm**

  Especifica la hora de inicio de la operación de programación. La hora de inicio de la programación debe

incluirse en el formato aaaa-MM-dd HH:mm.

- **-runasuser runasuser**

  Especifica si se va a cambiar el usuario de la operación de backup programada mientras se programa el backup.

- **-tasktaskspec**

  Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Debe proporcionarse la ruta completa del archivo XML, que proporciona la opción -taskspec .

El comando smo Storage list

Puede ejecutar el comando Storage list para mostrar la lista de sistemas de almacenamiento asociados con un perfil en particular.

Sintaxis

```
        smo storage list
-profile profile
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. El nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

Ejemplo

En el siguiente ejemplo se muestran los sistemas de almacenamiento asociados al perfil mjulian:

```
smo storage list -profile mjullian
```

```
Sample Output:
Storage Controllers
--------------------
FAS3020-RTP07OLD
```

El comando smo Storage rename

Este comando actualiza el nombre o la dirección IP del sistema de almacenamiento.

Sintaxis

```
        smo storage rename
-profile profile
-oldname old_storage_name
-newname new_storage_name
\[-quiet \| -verbose\]
```

Parámetros

- * perfil*

  Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-oldname old_storage_name**

  Especifica la dirección IP o el nombre del sistema de almacenamiento antes de cambiar el nombre del sistema de almacenamiento. Debe introducir la dirección IP o el nombre del sistema de almacenamiento que se muestra cuando se ejecuta el comando smo Storage list.

- **-newname new_storage_name**

  Especifica la dirección IP o el nombre del sistema de almacenamiento después de cambiar el nombre del sistema de almacenamiento.

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo

En el ejemplo siguiente se utiliza el comando smo Storage rename para cambiar el nombre del sistema de almacenamiento:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

El comando dump del sistema de smo

Puede ejecutar el comando system dump para crear un archivo JAR que contenga información de diagnóstico acerca del entorno del servidor.

Sintaxis

```
        smo system dump
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo del comando system dump

En el ejemplo siguiente se utiliza el comando dump del sistema de smo para crear un archivo JAR:

```
smo system dump
Path: C:\\userhomedirectory\\netapp\\smo\\3.3.0\\smo_dump_hostname.jar
```

El comando smo system verify

Este comando confirma que todos los componentes del entorno necesario para ejecutar SnapManager están configurados correctamente.

Sintaxis

```
        smo system verify
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo del comando system verify

En el ejemplo siguiente se usa el comando smo system verify.

```
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.
```

El comando version de smo

Puede ejecutar el comando version para determinar qué versión de SnapManager va a ejecutar en el host local.

Sintaxis

```
        smo version
\[-quiet \| -verbose\]
```

Parámetros

- **-silencio**

  Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

  Muestra la fecha de creación y el contenido de cada perfil. También muestra mensajes de error, advertencia e informativos en la consola.

Ejemplo del comando version

En el siguiente ejemplo, se muestra la versión de SnapManager:

```
smo version
SnapManager for Oracle Version: 3.3.1
```

Resolución de problemas de SnapManager

Puede encontrar información sobre algunos de los problemas más comunes que se pueden producir y el modo en que puede resolverlos.

La siguiente tabla describe los problemas comunes y las posibles soluciones:

Pregunta basada en cuestiones	Posible solución

¿Se están ejecutando la base de datos de destino y el listener?	Ejecute el comando lsnrctl status. Asegúrese de que la instancia de base de datos está registrada en el listener.
¿El almacenamiento está visible?	Siga estos pasos: 1. Haga clic con el botón derecho del ratón en Mi PC y, a continuación, seleccione **Administrar**. 2. Haga clic en **Storage** > **SnapDrive** > **Hostname** > **Disks**.
¿Se ejecuta el servidor SnapManager?	Compruebe el estado y, a continuación, inicie el servidor utilizando Configuración de servicio. Para poder utilizar la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) para iniciar comandos de la SnapManager relacionados con los perfiles, el servidor debe estar en ejecución. Puede crear o actualizar repositorios sin iniciar el servidor, pero para ejecutar todas las demás operaciones de SnapManager, el servidor debe estar en ejecución. Para iniciar el servidor SnapManager, introduzca el siguiente comando: SMO_Server start.
¿Son todos los componentes necesarios para ejecutar la configuración correcta de SnapManager?	Ejecute el comando smo system verify para comprobar que SnapDrive está configurado correctamente.
¿Tiene la versión correcta de SnapManager?	Use el comando version de smo para comprobar la versión de SnapManager.

¿Ha consultado los archivos de registro de SnapManager para determinar si los mensajes de error pueden ayudar a aislar el problema?	SnapManager registra todas las entradas de registro en un conjunto de archivos de registro giratorios. Los archivos de registro se encuentran en C:\Program_files\NetApp\SnapManager para Oracle\logs. Si utiliza Windows 2008, los registros se encuentran en las siguientes ubicaciones: • Registros de operaciones: ◦ C:\Archivos de programa\NetApp\SnapManager para Oracle\var\log\smo • Registros de cliente: ◦ C:\Users\Administrator\AppData\Roaming\NetApp\smo\3.3.0\ También puede ser útil consultar los registros en la siguiente ubicación: C:\Documents and Settings\hostname\Application Data\NetApp\smo\3.3.0\log Cada registro de operaciones se escribe en su propio archivo de registro con el formato smo_of_date_time.log.
Si tiene registros de archivos almacenados en un sistema de almacenamiento que no ejecuta Data ONTAP, ¿los ha excluido de tener en cuenta para backup con SnapManager?	El archivo smo.config permite excluir determinados archivos de registro de archivos. Para Windows, el archivo se encuentra en la siguiente ubicación: C:\Program_files\NetApp\smo\properties\smo.config Utilice el formato mencionado en el archivo para excluir los registros de archivo locales. Para obtener información adicional, consulte el tema "Configuración de propiedades de configuración". También puede excluir los destinos del registro de archivos mientras crea un backup desde la interfaz de línea de comandos de SnapManager. Para obtener información adicional, consulte el tema «"creación de copias de seguridad de bases de datos". También puede excluir los destinos del registro de archivos al crear un backup desde la interfaz gráfica de usuario de SnapManager.

¿Tiene abierta una ventana de MS-dos en el directorio en el que intenta instalar o actualizar SnapManager en Windows?	Verá un mensaje de error similar al siguiente: `Directory C:\Program Files\NetApp\SnapManager for Oracle\bin is currently in use by another program`. Cualquier ventana, abierta por usted u otro usuario, que haga referencia actualmente a este directorio debe cerrarse antes de que pueda continuar la instalación. Cierre la ventana e intente realizar la instalación o la actualización de nuevo.
¿No ha podido conectarse al repositorio?	Si la conexión a un repositorio falla, ejecute el comando lsnrctl status en la base de datos del repositorio y compruebe los nombres de servicio activos. Cuando SnapManager se conecta a la base de datos del repositorio, utiliza el nombre de servicio de la base de datos. Dependiendo de cómo esté configurado el listener, este puede ser el nombre corto del servicio o el nombre completo del servicio. Cuando SnapManager se conecta a una base de datos para una operación de backup, restauración u otra, utiliza el nombre de host y el SID. Si el repositorio no se inicializa correctamente porque no se puede acceder a él actualmente, recibe un mensaje de error que le pregunta si desea quitar el repositorio. Es posible quitar el repositorio de la vista actual para poder realizar operaciones en otros repositorios. Además, compruebe si el servicio correspondiente se está ejecutando.
¿El sistema puede resolver el nombre de host?	Compruebe si el nombre de host especificado está en una subred diferente. Si recibe un mensaje de error indicando que SnapManager no puede resolver el nombre de host, añada el nombre de host en el archivo de host. Añada el nombre de host al archivo ubicado en C:\WINDOWS\system32\drivers\etc\hosts: xxx.xxx.xxx.xxx hostname IP address
¿Se ejecuta SnapDrive?	Para ver el estado de SnapDrive, vaya a Servicios y, a continuación, seleccione el servicio SnapDrive.
¿A qué sistemas de almacenamiento se ha configurado para acceder mediante SnapDrive?	Para encontrar los sistemas de almacenamiento configurados para SnapDrive, realice los siguientes pasos: 1. Haga clic con el botón derecho del ratón en **Mi PC** y, a continuación, seleccione **Administrar**. 2. Haga clic en **almacenamiento** > **SnapDrive**. 3. Haga clic con el botón derecho del ratón en el nombre de host y, a continuación, seleccione **Ajustes del protocolo de transporte**.

¿Cómo se puede mejorar el rendimiento de la interfaz gráfica de usuario de SnapManager?	• Asegúrese de tener credenciales de usuario válidas para el repositorio, el host de perfiles y el perfil. Si la credencial no es válida, borre las credenciales de usuario para el repositorio, el host del perfil y el perfil. Restablezca las mismas credenciales de usuario que haya establecido antes para el repositorio, el host del perfil y el perfil. Para obtener información adicional acerca de cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales después de borrar la caché de credenciales". • Cierre los perfiles no utilizados. Si el número de perfiles que ha abierto es mayor, el rendimiento de la interfaz gráfica de usuario de SnapManager se ralentiza. • Compruebe si ha activado **Abrir al inicio** en la ventana Preferencias del usuario en el menú **Admin** desde la GUI de SnapManager. Si esto está habilitado, el archivo de configuración de usuario (user.config) disponible en C:\Documents and Settings\Administrator\Application Data\NetApp\smo\3.3.0\gui\state se muestra como openOnStartup=PROFILE. Debido a que **Abrir al inicio** está activado, debe buscar perfiles abiertos recientemente desde la GUI de SnapManager, utilizando lastOpenProfiles en el archivo de configuración de usuario (user.config): LastOpenProfiles=PROFILE1,PROFILE2,PROFILE3,… Puede eliminar los nombres de perfil que aparecen y mantener siempre un número mínimo de perfiles abiertos. • Antes de instalar la nueva versión de SnapManager en el entorno basado en Windows, elimine las entradas del cliente de SnapManager disponibles en la siguiente ubicación: C:\Documents and Settings\Administrator\Application Data\NetApp

La interfaz gráfica de usuario de SnapManager tarda más tiempo en actualizarse cuando se SnapManager inician y se ejecutan simultáneamente en segundo plano. Al hacer clic con el botón derecho en el backup (que ya se ha eliminado pero se sigue mostrando en la interfaz gráfica de usuario de SnapManager), las opciones de backup para ese backup no se habilitan en la ventana Backup o Clone.	Debe esperar hasta que se actualice la interfaz gráfica de usuario de SnapManager y, a continuación, comprobar el estado de backup.
¿Qué haría si la base de datos de Oracle no está configurada en inglés?	Se pueden producir errores en las operaciones de SnapManager si el idioma de una base de datos de Oracle no está establecido en inglés.defina el idioma de la base de datos de Oracle en inglés: 1. Compruebe que la variable de entorno NLS_Lang no está establecida: Echo%NLS_Lang% 2. Añada la siguiente línea al archivo wrapper.conf ubicado en C:\SnapManager_install_directory\service: Set.NLS_Lang=AMERICAN_AMERICA.WE8MSWIN1252 3. Reinicie el servidor SnapManager: se reinicia smo_Server Si la variable de entorno del sistema está establecida en NLS_Lang, debe editar la secuencia de comandos para que no sobrescriba NLS_Lang.

¿Qué se haría si se produce un error en la operación de programación de backups si la base de datos del repositorio apunta a más de una IP y cada IP tiene un nombre de host diferente?	1. Detenga el servidor SnapManager. 2. Elimine los archivos de programación del directorio de repositorios de los hosts en los que desea activar la programación de backup. Los nombres de los archivos de programación pueden tener los siguientes formatos: ◦ repository#repo_username#repository_database_name#repository_host#repo_port ◦ Repository-repo_usernamereppository_database_name-repository_host-repo_Port **Nota:** debe asegurarse de que elimine el archivo de programa en el formato que coincida con los detalles del repositorio. 3. Reinicie el servidor SnapManager. 4. Abra otros perfiles en el mismo repositorio de la interfaz gráfica de usuario de SnapManager para asegurarse de que no se pierda ninguna información de programación de dichos perfiles.
¿Qué haría si la operación de SnapManager presenta un error de bloqueo del archivo de credenciales?	SnapManager bloquea el archivo de credenciales antes de la actualización y lo desbloquea después de la actualización.cuando se ejecutan varias operaciones a la vez, una de las operaciones puede bloquear el archivo de credenciales para actualizarlo. Si otra operación intenta acceder al archivo de credenciales bloqueadas al mismo tiempo, la operación genera un error de bloqueo de archivo. Configure los siguientes parámetros en el archivo smo.config en función de la frecuencia de las operaciones simultáneas: • FileLock.RetryInterval = 100 milisegundos • FileLock.timeout = 5000 milisegundos Los valores asignados a los parámetros deben ser en milisegundos.

¿Qué haría si el estado intermedio de la operación de verificación de backup muestra un error en la pestaña Monitor aunque todavía esté en ejecución la operación de verificación de backup?	El mensaje de error se registra en el archivo sm_gui.log. Debe buscar en el archivo de registro para determinar los nuevos valores de operation.heartbeatInterval and operation.heartbeatThreshold que resolverán este problema. 1. Añada los siguientes parámetros en el archivo smo.config: ◦ Operation.heartbeatInterval = 5000 ◦ Operation.heartbeatThreshold = 5000 el valor predeterminado asignado por SnapManager es 5000. 2. Asigne nuevos valores a estos parámetros. Los valores asignados a los parámetros deben ser en milisegundos. 3. Reinicie el servidor SnapManager y vuelva a realizar la operación.
¿Qué se debe hacer cuando se encuentra un problema de espacio en montón?	Cuando encuentre un problema de espacio en montón durante las operaciones de SnapManager para Oracle, debe realizar los siguientes pasos: 1. Desplácese hasta el directorio de instalación de SnapManager para Oracle. 2. Abra el archivo Launchjava desde la ruta installationdirectory\bin\Launchjava. 3. Aumente el valor del parámetro java -Xmx160m Java heap-space. Por ejemplo, puede aumentar el valor predeterminado de 160 m a 200 m. Si ha aumentado el valor del parámetro Java heap-space en las versiones anteriores de SnapManager para Oracle, debe conservar ese valor.

¿Qué haría si los servicios de SnapManager no se iniciaran en un entorno de Windows y aparece el siguiente mensaje de error: Windows no pudo iniciar Snap Manager en un equipo local. Para obtener más información, consulte el registro de eventos del sistema. Si se trata de un servicio que no es de Microsoft, póngase en contacto con el proveedor del servicio técnico y consulte el código de error 1 específico del servicio.	Configure los siguientes parámetros en el archivo wrapper.conf ubicado en Installation_directory\service. • El parámetro wrapper startup startup define el tiempo máximo permitido entre el contenedor que inicia Java Virtual Machine (JVM) y la respuesta de la JVM que ha iniciado la aplicación. El valor predeterminado se establece en 90 segundos. Sin embargo, es posible cambiar un valor superior a 0. Si especifica un valor no válido, se utiliza el valor predeterminado en su lugar. • El parámetro wrapper.timeout define el tiempo máximo permitido entre el contenedor haciendo ping a JVM y la respuesta de JVM. El valor predeterminado se establece en 90 segundos. Sin embargo, puede cambiar a un valor mayor que 0. Si especifica un valor no válido, se utiliza el valor predeterminado en su lugar.

Volcar archivos

Los archivos de volcado son archivos de registro comprimidos que contienen información acerca de SnapManager y su entorno. Los diferentes tipos de archivos de registro creados son operación, perfil y archivo de volcado del sistema.

Puede utilizar el comando dump o la ficha **Create Diagnostics** de la interfaz gráfica de usuario (GUI) para recopilar información sobre una operación, un perfil o el entorno. Un volcado del sistema no requiere un perfil; sin embargo, los volcados de perfil y operación requieren perfiles.

SnapManager incluye la siguiente información de diagnóstico en el archivo de volcado:

- Los pasos realizados
- El tiempo que tarda cada paso en completarse
- El resultado de cada paso
- Error, si hay alguno, que ocurrió durante la operación

> Los archivos de registro o los archivos de volcado de SnapManager permiten permisos de lectura y escritura sólo para los usuarios raíz y los demás usuarios que pertenecen al grupo de usuarios raíz.

SnapManager también incluye la siguiente información en el archivo:

- Arquitectura y versión del sistema operativo
- Variables de entorno

- Versión de Java
- Arquitectura y versión de SnapManager
- Preferencias de SnapManager
- Mensajes de SnapManager
- propiedades log4j
- Arquitectura y versión de SnapDrive
- Archivos de registro de SnapDrive
- Versión de Oracle
- Detalles del inventario local de Oracle OPatch
- Versión de Oracle de la base de datos del repositorio
- Tipo de base de datos de destino (independiente)
- Función de base de datos de destino (primaria, física en espera o lógica en espera)
- Configuración de Oracle Recovery Manager (RMAN) de la base de datos de destino (sin integración de RMAN, RMAN con archivos de control o RMAN con archivo de catálogo)
- Versión de Oracle de la base de datos de destino
- Identificador del sistema (SID) de la base de datos de destino
- Nombre de la base de datos RMAN y nombre de la conexión TNS
- Nombre del servicio de base de datos del repositorio
- Instancias de base de datos instaladas en el host
- Descriptor perfil
- Memoria compartida máxima
- Intercambie información de espacio
- Información de la memoria
- Entorno multivía
- Versión de utilidades de host
- Versión del software del iniciador de la interfaz de sistemas para equipos pequeños de Microsoft Internet (iSCSI) para Windows
- Resultado del comando system verify

El archivo de volcado también enumera las limitaciones de SnapManager en Windows.

Los archivos de volcado de SnapManager también contienen el archivo de recopilador de datos de SnapDrive y el archivo de registro de alertas de Oracle. Puede recopilar el archivo de registro de alertas de Oracle mediante los comandos de volcado de la operación smo y de volcado de perfiles de smo.

> El volcado del sistema no contiene registros de alertas de Oracle; sin embargo, los volcados de alerta y de operación contienen los registros de alerta.

Aunque no se esté ejecutando el servidor host SnapManager, puede acceder a la información de volcado mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario.

Si se encuentra con un problema que no se puede resolver, puede enviar estos archivos a los servicios

globales de NetApp.

Creación de archivos de volcado en el nivel de las operaciones

Puede utilizar el comando de volcado de la operación de smo con el nombre o el ID de la operación fallida para obtener información del registro sobre una operación en particular. Es posible especificar niveles de registro diferentes para recopilar información sobre una operación, un perfil, un host o un entorno específicos.

1. Introduzca el siguiente comando: Volcado de operación de smo -idguid

> El comando smo operation dump proporciona un superconjunto de la información proporcionada por el comando de volcado de perfil de smo, que a su vez proporciona un superconjunto de la información proporcionada por el comando de volcado del sistema smo.

Ubicación del archivo de volcado:

```
Path:\<user-home>\Application
Data\NetApp\smo\3.3.0\smo_dump_8abc01c814649ebd0114649ec69d0001.jar
```

Creación de archivos de volcado a nivel de perfil

Puede encontrar información de registro sobre un perfil determinado mediante el comando smo profile dump con el nombre del perfil.

1. Introduzca el siguiente comando: Volcado de perfil de smo -profile profile profile_name

Ubicación del archivo de volcado:

```
Path:\<user-home>\Application
Data\NetApp\smo\3.3.0\smo_dump_8abc01c814649ebd0114649ec69d0001.jar
```

> Si se produce un error al crear un perfil, utilice el comando smosystem dump. Una vez que haya creado correctamente un perfil, utilice los comandos de volcado de operación smooperation y de volcado de moporofile.

Creación de archivos de volcado en el nivel del sistema

Puede usar el comando de volcado del sistema smo para obtener información sobre el registro del entorno y el host de SnapManager. Es posible especificar niveles de registro diferentes para recoger información sobre una operación, un perfil o un host y un entorno específicos.

1. Introduzca el siguiente comando: Volcado de sistema smo

Volcado resultante

```
Path:\<user-home>\Application
Data\NetApp\smo\3.3.0\smo_dump_server_host.jar
```

Cómo localizar archivos de volcado

El archivo de volcado se encuentra en el sistema cliente para facilitar el acceso. Estos archivos son útiles si necesita solucionar un problema relacionado con el perfil, el sistema o cualquier operación.

El archivo de volcado se encuentra en el directorio principal del usuario en el sistema cliente.

- Si utiliza la interfaz gráfica de usuario (GUI), el archivo de volcado se encuentra en:

```
user_home\Application Data\NetApp\smo\3.3.0\smo_dump dump_file_type_name
server_host.jar
```

- Si utiliza la interfaz de línea de comandos (CLI), el archivo de volcado se encuentra en:

```
user_home\.netapp\smo\3.3.0\smo_dump_dump_file_type_name server_host.jar
```

El archivo dump contiene el resultado del comando dump. El nombre del archivo depende de la información proporcionada. En la siguiente tabla se muestran los tipos de operaciones de volcado y los nombres de archivo resultantes:

Tipo de operación de volcado	Nombre de archivo resultante
Comando de volcado de la operación con ID de operación	smo_dump_operation-id.jar

Comando de volcado de la operación sin ID de operación	Se muestra la siguiente salida de volcado de la operación de smo -profile VH1-verbose:
	`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`

Comando system dump	smo_dump_host-name.jar
Comando de volcado de perfil	smo_dump_profile-name_host-name.jar

Cómo recopilar archivos de volcado

Es posible incluir -dump en el comando SnapManager para recoger los archivos de volcado después de una operación de SnapManager correcta o con errores.

Es posible recoger archivos de volcado para las siguientes operaciones de SnapManager:

- Creación de perfiles
- Actualizando perfiles
- Crear backups
- Verificación de backups
- Eliminar backups
- Liberando backups
- Montar backups
- Desmontaje de backups
- Restaurar backups
- Crear clones
- Eliminar clones

> Al crear un perfil, puede recopilar archivos de volcado sólo si la operación se realiza correctamente. Si se produce un error al crear un perfil, debe utilizar el comando de volcado del sistema smsystem. Para que los perfiles se realicen correctamente, puede utilizar los comandos de volcado smooperation y smoprofile para recopilar los archivos de volcado.

ejemplo

```
      smo  backup create -profile targetdb1_prof1 -auto -full -online
-dump
```

Recopilación de información de registro adicional para facilitar la depuración

Si necesita registros adicionales para depurar una operación de SnapManager con errores, debe configurar una variable de entorno externa Server.log.level. Esta variable anula el nivel de registro predeterminado y vuelca todos los mensajes de registro del archivo de registro. Por ejemplo, puede cambiar el nivel de registro a DEBUG, lo que registra mensajes adicionales y puede ayudar en la depuración de problemas.

Los registros de SnapManager se pueden encontrar en las siguientes ubicaciones:

- SnapManager_install_Directory\log

Para anular el nivel de registro predeterminado, debe realizar los siguientes pasos:

1. Cree un archivo de texto platform.override en el directorio de instalación de SnapManager.
2. Agregue el parámetro Server.log.level en el archivo de texto platform.override.
3. Asignar un valor (SEGUIMIENTO, DEPURACIÓN, INFO, WARN, ERROR, FATAL o PROGRESS) en el parámetro Server.log.level.

   Por ejemplo, para cambiar el nivel de registro a ERROR, establezca el valor Server.log.level en ERROR.

   Server.log.level=ERROR

4. Reinicie el servidor SnapManager.

> Si no se necesita la información adicional del registro, puede eliminar el parámetro Server.log.level del archivo de texto platform.override.

SnapManager gestiona el volumen de archivos de registro del servidor según los valores definidos por el usuario de los siguientes parámetros en el archivo smo.config:

- log.max_log_files
- log.max_log_file_size
- log.max_rolling_operation_factory_logs

Solucionar problemas de clones

Puede encontrar información sobre eso que puede ocurrir durante las operaciones de clonado y cómo puede resolverla.

Síntoma	Explicación	Solución alternativa
Se produce un error en la operación de clonado cuando el destino de archivado está establecido en USE_DB_RECOVERY_FILE_DEST.	Cuando el destino de archivado hace referencia a USE_DB_RECOVERY_FILE_DEST, el área de recuperación flash (FRA) gestiona activamente el registro de archivos. SnapManager no utiliza la ubicación de la FRA durante las operaciones de clonado o restauración y, por lo tanto, fallan las operaciones.	Cambie el destino de archivado por la ubicación del registro de archivos real en lugar de la ubicación del FRA.

Se produce un error en la operación de clonado con el siguiente mensaje de error: Cannot Perform: Clone Create. Causa raíz: ORACLE-00001: Error al ejecutar SQL: [ALTER DATABASE OPEN RESETLOGS;]. El comando devolvió: ORA-01195: El backup en línea del archivo 1 necesita más recuperación para ser coherente.	Este problema ocurre si Oracle listener no puede conectarse a la base de datos.	Si utiliza la interfaz gráfica de usuario de SnapManager para clonar un backup, realice las siguientes acciones: 1. En el árbol del repositorio, haga clic en **repositorio** > **Host** > **Perfil** para visualizar las copias de seguridad. 2. Haga clic con el botón derecho del ratón en la copia de seguridad que desea clonar y seleccione **Clonar**. 3. En la página Clone Initialization, introduzca los valores obligatorios y seleccione el método de especificación del clon. 4. En la página Clone Specification, seleccione **parámetros**. 5. Haga clic en la ficha **+parámetro**. 6. En el campo **Nombre de parámetro**, introduzca el nombre como local_listener y haga clic en **Aceptar**. 7. Active la casilla de verificación **Anular valor predeterminado** de la fila local_listener. 8. Haga clic en cualquier parámetro y, a continuación, haga doble clic en el parámetro local_listener e introduzca el siguiente valor:(ADDRESS=(PROTOCOL=TCP)(HOST=<your_host_name>)(PORT=<port#>))) 9. Haga clic en **Guardar en archivo**. 10. Haga clic en **Siguiente** y continúe con el asistente de creación de clones. Si está utilizando CLI para clonar una copia de seguridad, debe incluir la siguiente información en la etiqueta **<parameters>** del archivo de especificación del clon:

Se produce un error en la operación de clonado con un mensaje de error que indica que el punto de montaje que está usando ya está en uso.	SnapManager no permite montar un clon en un punto de montaje existente. Por lo tanto, un clon incompleto no eliminaba el punto de montaje.	Especifique otro punto de montaje para que lo utilice el clon, o desmonte el punto de montaje problemático.
Se produce un error en la operación de clonado con un mensaje de error acerca de los archivos de datos que no tienen la extensión .dbf.	Algunas versiones de la utilidad Oracle NID no funcionan con archivos de datos a menos que los archivos utilicen una extensión .dbf.	• Cambie el nombre del archivo de datos para darle una extensión .dbf. • Repita la operación de backup. • Clone el backup nuevo.
Se produce un error en la operación de clonado debido a requisitos no cumplidos.	Está intentando crear un clon; sin embargo, no se cumplieron algunos de los requisitos previos.	Proceda como se describe en *creando un clon* para cumplir con los requisitos previos.
SnapManager para Oracle no puede clonar bases de datos físicas de Oracle 10gR2 (10.2.0.5) en espera de Oracle Data Guard.	SnapManager para Oracle no deshabilita el modo de recuperación gestionado mientras se realiza un backup sin conexión de las bases de datos físicas en espera de Oracle 10gR2 (10.2.0.5) creadas con los servicios de Oracle Data Guard. Debido a este problema, el backup sin conexión realizado no es coherente. Cuando SnapManager para Oracle intenta clonar el backup sin conexión, ni siquiera intenta realizar una recuperación en la base de datos clonada. Como el backup no es coherente, la base de datos clonada requiere una recuperación y, por lo tanto, Oracle no puede crear el clon correctamente.	Actualización de la base de datos Oracle a Oracle 11gR1 (parche 11.1.0.7).

Solución de problemas de la interfaz gráfica de usuario

Es posible encontrar información sobre algunos problemas de la interfaz gráfica de usuario (GUI) conocidos comunes que pueden ser de ayuda para resolverlos.

Problema	Explicación	Solución alternativa

Al acceder a la GUI de SnapManager para realizar una operación, puede aparecer el siguiente mensaje de error: SMO-20111 : error de autenticación para el usuario en el host.	Este problema se produce si se cambia la contraseña del usuario en el host en el que se ejecuta el servidor SnapManager.después de cambiar la contraseña, la caché de credenciales creada para el usuario que inició la GUI deja de ser válida. La interfaz gráfica de usuario de SnapManager sigue utilizando las credenciales de la caché para autenticar y, por lo tanto, la autenticación falla.	Debe realizar una de las siguientes tareas: • Elimine las credenciales del usuario cuya contraseña se modificó y añada las nuevas credenciales en la caché ejecutando los siguientes comandos: a. eliminación de la credencial de smo b. se han establecido credenciales de smo • Borrar toda la caché ejecutando el comando clear de credenciales de smo. Vuelva a abrir la GUI y establezca las credenciales, si se le solicita.
Se muestra una advertencia de seguridad mientras se utiliza Java Web Start para acceder a la GUI de SnapManager.	Al acceder a la GUI de SnapManager mediante Java Web Start, se muestra una advertencia de seguridad.este problema se produce porque los tarros JNLP son autofirmados y la versión Java utilizada por SnapManager no permite los tarros autofirmados en un nivel de seguridad alto.	Cambie la configuración de seguridad a medio en el panel de control de Java o agregue la dirección URL de la GUI de SnapManager a la lista de excepciones.
La interfaz gráfica de usuario de inicio web de SnapManager muestra la versión incorrecta.	Después de cambiar a SnapManager de una versión posterior a una versión anterior al iniciar la GUI de inicio web, se inicia la versión posterior de la GUI de inicio web de SnapManager.	También debe borrar la caché realizando los siguientes pasos: 1. Haga clic en **Inicio** y seleccione **Ejecutar**. 2. Introduzca lo siguiente: Javaws -viewer 3. En la pantalla del visor de caché Java, haga clic con el botón derecho del ratón en la aplicación SnapManager y seleccione **Eliminar**.

Al reiniciar la GUI e intentar comprobar las copias de seguridad de un perfil determinado, sólo verá los nombres de los perfiles.	SnapManager no muestra ninguna información sobre un perfil hasta que lo abre.	Siga estos pasos: 1. Haga clic con el botón derecho del ratón en el perfil y seleccione **Abrir** en el menú. SnapManager muestra el cuadro de diálogo autenticación de perfiles. 2. Introduzca el nombre de usuario y la contraseña del host. SnapManager muestra la lista de backups. Sólo es necesario autenticar el perfil una vez, siempre que las credenciales sean válidas y permanezcan en la caché.
La instalación de la GUI en Windows se realiza correctamente, pero con errores.	La cuenta de usuario utilizada para instalar la GUI no tiene permisos suficientes para configurar los iconos y accesos directos para todos los usuarios. La cuenta de usuario no tiene permisos para modificar el directorio C:\Documents and Settings\All Users.	• Vuelva a instalar la GUI con ajustes diferentes. En elegir disponibilidad de iconos, desactive la casilla de verificación **hacer que estos accesos directos estén disponibles para todos los usuarios de este PC**. • Inicie sesión con una cuenta de usuario que no esté restringida y vuelva a instalar la GUI.
Al abrir el primer repositorio en la GUI, aparece un mensaje de error similar al siguiente: El nombre de perfil XXXX choca con el repositorio cargado previamente.	Los perfiles con el mismo nombre no pueden existir en un repositorio. Además, solo es posible abrir un repositorio a la vez.	Haga referencia a los perfiles en conflicto de dos usuarios de sistema operativo (SO) diferentes o cambie el nombre del perfil emitiendo una sentencia SQL para el repositorio: ACTUALIZAR SMO_33_PROFILE SET NAME = 'NEW_NAME' DONDE NAME = 'OLD_NAME'

Se muestra un mensaje de error similar al siguiente: SMO-01092: No se puede inicializar la repo1@ del repositorio no existe:repo1SMO-11006: No se puede resolver el host no existe	El repositorio es inaccesible, quizás porque ya no existe. La GUI inicializa la lista de repositorios desde el archivo de credenciales.	El mensaje de error le pregunta si desea eliminar este repositorio para que no se intente cargarlo en el futuro. Si no necesita acceder a este repositorio, haga clic en **Eliminar** para eliminarlo de la vista GUI. Esto elimina la referencia al repositorio en el archivo de credenciales y la interfaz gráfica de usuario no intenta volver a cargar el repositorio.
SnapManager tarda más tiempo en cargar la estructura del árbol de la base de datos y da como resultado un mensaje de error de tiempo de espera que se muestra en la interfaz gráfica de usuario de SnapManager.	Cuando se intenta realizar una operación de backup parcial desde la interfaz gráfica de usuario de SnapManager, SnapManager intenta cargar las credenciales para todos los perfiles y, si hay entradas no válidas, SnapManager intenta validar la entrada y esto provoca que se muestre un mensaje de error de tiempo de espera.	Elimine las credenciales del host, el repositorio y el perfil que no utilice el comando credential delete de la interfaz de línea de comandos (CLI) de SnapManager.
Los scripts personalizados para el procesamiento previo o posterior a la actividad que se realizan antes o después de las operaciones de backup, restauración o clonado no se pueden ver en la interfaz gráfica de usuario de SnapManager.	Cuando se añaden scripts personalizados en la ubicación del backup, la restauración o la clonado de scripts después de iniciar el asistente respectivo, los scripts personalizados no se muestran en la lista Available Scripts.	Reinicie el servidor host SnapManager y, a continuación, abra la interfaz gráfica de usuario de SnapManager.
No se puede utilizar el archivo XML de especificación del clon creado en SnapManager (3.1 o anterior) para la operación de clonado.	Desde SnapManager 3.2 para Oracle, la sección de especificación de tareas (especificación de tareas) se proporciona como un archivo XML de especificación de tareas independiente.	Si utiliza SnapManager 3.2 para Oracle, debe eliminar la sección de especificación de tareas del XML de especificación del clon o crear un archivo XML de especificación del clon nuevo.SnapManager 3.3 o posterior no admite el archivo XML de especificación del clon creado en SnapManager 3.2 o versiones anteriores.

El funcionamiento de SnapManager en la GUI no se realiza después de haber borrado las credenciales de usuario mediante el comando smo credential clear desde la CLI de SnapManager o haciendo clic en **Admin** > **credenciales** > **Borrar** > **caché** desde la interfaz gráfica de usuario de SnapManager.	Se borran las credenciales establecidas para los repositorios, hosts y perfiles. SnapManager verifica las credenciales de usuario antes de iniciar cualquier operación.cuando las credenciales de usuario no son válidas, SnapManager no puede autenticarse. Cuando se elimina un host o un perfil del repositorio, las credenciales del usuario siguen estando disponibles en la caché. Estas entradas de credenciales innecesarias ralentizan las operaciones de SnapManager de la interfaz gráfica de usuario.	Reinicie la interfaz gráfica de usuario de SnapManager en función de cómo se borre la caché. **Nota:** • Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager. • Si borró la caché de credenciales de la interfaz gráfica de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager. • Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar la interfaz gráfica de usuario de SnapManager. Configure las credenciales que haya otorgado para el repositorio, el host del perfil y el perfil. Desde la GUI de SnapManager, si no hay ningún repositorio asignado en el árbol de repositorios, realice los siguientes pasos: 1. Haga clic en **tareas** > **Añadir repositorio nuevo** 2. Haga clic con el botón derecho del ratón en el repositorio, haga clic en **Abrir** e introduzca las credenciales de usuario en la ventana **autenticación de credenciales de repositorio**. 3. Haga clic con el botón derecho del ratón en el host bajo el repositorio, haga clic en **Abrir** e introduzca las credenciales de usuario en **autenticación de credenciales de host**. 4. Haga clic con el botón derecho del ratón en el perfil bajo el host, haga clic en **Abrir** e introduzca las credenciales de usuario en **autenticación de credenciales de perfil**.

No se puede abrir la GUI de SnapManager mediante la GUI de inicio web de Java debido a la fortaleza del cifrado de capa de sockets seguros (SSL) más débil del explorador.	SnapManager no admite cifrados SSL de más de 128 bits.	Actualice la versión del navegador y compruebe la intensidad del cifrado.

Resolución de problemas conocidos

Es necesario conocer algunos problemas conocidos que se pueden producir al utilizar SnapManager y cómo solucionar sus problemas.

SnapManager para Oracle no identifica los perfiles de modo Cluster

Si el nombre del perfil de Cluster-Mode no está presente en el archivo cmode_profiles.config del directorio de instalación de SnapManager para Oracle, el siguiente mensaje de error podría activarse:

Configure el servidor DFM mediante la configuración de SnapDrive set -dfm user_name Appliance_name.

Además, al actualizar SnapManager para Oracle, si elimina la carpeta /opt/NetApp/smo/*, el archivo cmode_profiles.config que tiene los nombres de perfil de Cluster-Mode también se elimina. Este problema también activa el mismo mensaje de error.

Solución

Actualice el perfil: <profile_name> de perfil de actualización de smo

> Si se instala SnapManager para Oracle en la ruta /opt/NetApp/smo/, la ubicación del archivo es /opt/NetApp/smo/cmode_profile/cmode_profiles.config.

El servidor no se inicia

Al iniciar el servidor, es posible que aparezca un mensaje de error similar al siguiente:

SMO-01104: Error al invocar el comando: SMO-17107: El servidor SnapManager no se pudo iniciar en el puerto 8074 debido a los siguientes errores: La dirección java.net.BindException: ya está en uso

Esto puede deberse a que los puertos de escucha SnapManager (27214 y 27215, de forma predeterminada) están actualmente en uso en otra aplicación.

Este error también puede ocurrir si el comando smo_Server ya se está ejecutando, pero SnapManager no detecta el proceso existente.

Solución

Es posible volver a configurar SnapManager o la otra aplicación para utilizar diferentes puertos.

Para volver a configurar SnapManager, edite el siguiente archivo: C:\Program Files\NetApp\SnapManager para Oracle\properties\smo.config

Asigne los siguientes valores:

- Servidor de SMO.Port=27214
- Servidor SMO.rmiRegistry.Port=27215
- remote.registry.ocijdbc.port= 27215

  El archivo remote.registry.ocijdbc.Port debe ser el mismo que Server.rmiRegistry.Port.

Para iniciar el servidor SnapManager, realice los siguientes pasos:

1. Haga clic en **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. Puede iniciar el servidor de una de estas tres formas:
   - En el panel izquierdo, haga clic en **Inicio**.
   - Haga clic con el botón derecho en NetApp SnapManager 3.3 for Oracle y seleccione **Inicio** en el menú desplegable.
   - Haga doble clic en NetApp SnapManager 3.3 for Oracle y, en la ventana Propiedades que se abrirá, haga clic en **Inicio**.

No se pueden gestionar los nombres de destino de los archivos de registro de archivos si los nombres de destino forman parte de otros nombres de destino

Al crear una copia de seguridad del registro de archivos, si el usuario excluye un destino que forme parte de otros nombres de destino, también se excluirán los demás nombres de destino.

Por ejemplo, supongamos que hay tres destinos disponibles para ser excluidos: E:\\Arch, G:\\Arch y H:\\Arch. Al crear la copia de seguridad del archivo de registro de archivos, si excluye E:\\Arch mediante el comando

```
smo backup create -profile almsamp1 -data -online -archivelogs  -exclude
-dest E:\\arch
```

, SnapManager para Oracle excluye todos los destinos a partir de E:\\Arch.

Solución

- Agregue un separador de ruta después de que los destinos estén configurados en v$archive_dest. Por ejemplo, cambie E:\\Arch a E:\\Arch\.
- Al crear una copia de seguridad, incluya destinos en lugar de excluir cualquier destino.

El tamaño de la base de datos del repositorio crece con el tiempo y no con el número de backups

El tamaño de la base de datos del repositorio crece con el tiempo debido a que las operaciones SnapManager insertan o eliminan datos dentro del esquema en las tablas de la base de datos del repositorio, lo que da como resultado un uso elevado del espacio de índice.

Solución

Debe supervisar y reconstruir los índices de acuerdo con las directrices de Oracle para controlar el espacio consumido por el esquema del repositorio.

No se puede acceder a la interfaz gráfica de usuario de SnapManager y se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva

Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

En la siguiente tabla, se enumeran las diferentes acciones que se pueden realizar y sus excepciones:

Operaciones	Excepciones
Abrir un repositorio cerrado	El siguiente mensaje de error se registra en sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: Closed Connection java.sql.SQLException: Closed Connection.
Para actualizar un repositorio abierto, pulse F5	Se muestra una excepción de repositorio en la GUI y también registra una NullPointerException en el archivo sm_gui.log.
Actualizar el servidor host	Se registra una NullPointerException en el archivo sumo_gui.logl.
Creación de un nuevo perfil	Aparecerá NullPointerException en la ventana Profile Configuration.
Actualizar un perfil	La siguiente excepción SQL se registra en sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: Closed Connection.
Obtener acceso a un backup	El siguiente mensaje de error se registra en sm_gui.log: No se pudo inicializar de forma lazilada una colección.
Ver las propiedades de clon	El siguiente mensaje de error se registra en sm_gui.log y sumo_gui.log: No se pudo inicializar de forma lazilada una colección.

Solución

Debe asegurarse de que se ejecute la base de datos del repositorio cuando se desea acceder a la interfaz gráfica de usuario o realizar cualquier operación de SnapManager.

No se pueden crear los archivos temporales para la base de datos clonada

Cuando los archivos de espacio de tabla temporales de la base de datos de destino se colocan en puntos de montaje diferentes del punto de montaje de los archivos de datos, la operación de creación de clonado se realiza correctamente, pero SnapManager no puede crear archivos temporales para la base de datos clonada.

Solución

Debe realizar una de las siguientes acciones:

- Asegúrese de que la base de datos de destino esté diseñada para que los archivos temporales se coloquen en el mismo punto de montaje que los archivos de datos.
- Crear manualmente o añadir archivos temporales en la base de datos clonada.

Se produce un error en el backup de la base de datos Data Guard en espera

Si se configura alguna ubicación de registro de archivos con el nombre de servicio de la base de datos primaria, se produce un error en el backup de la base de datos en espera de Data Guard.

Solución

En la GUI, debe desactivar **especificar la ubicación del registro de archivo externo** correspondiente al nombre de servicio de la base de datos primaria.

Se produce un error en la ejecución de varias operaciones paralelas en SnapManager

Cuando se ejecutan varias operaciones en paralelo en bases de datos independientes que residen en el mismo sistema de almacenamiento, el igroup para LUN asociadas con ambas bases de datos puede eliminarse debido a una de las operaciones. Más adelante, si la otra operación intenta utilizar el igroup eliminado, SnapManager muestra un mensaje de error.

Por ejemplo, si ejecuta las operaciones de eliminación de backup y creación de backup en bases de datos diferentes casi al mismo tiempo, la operación de creación de backup generará errores. Los siguientes pasos secuenciales muestran lo que ocurre cuando se ejecutan operaciones de eliminación de backup y creación de backup en distintas bases de datos casi al mismo tiempo.

1. Ejecute el comando backup delete.
2. Ejecute el comando backup create.
3. El comando backup create identifica el igroup ya existente y utiliza el mismo igroup para asignar la LUN.
4. El comando backup delete elimina la LUN de backup, que se asignó al mismo igroup.
5. A continuación, el comando backup delete elimina el igroup porque no hay ninguna LUN asociada con el igroup.
6. El comando backup create crea el backup e intenta asignar al igroup que no existe y, por lo tanto, se produce un error en la operación.

Qué hacer

Debe crear un igroup para cada sistema de almacenamiento que utilice la base de datos mediante el siguiente comando: Sdcli igroup create

No se puede restaurar la base de datos de RAC desde uno de los nodos de RAC donde no se creó el perfil

En un entorno de Oracle RAC donde ambos nodos pertenecen al mismo clúster, si se intenta realizar una operación de restauración desde un nodo que es diferente del nodo donde se creó el backup, se produce un error en la operación de restauración.

Por ejemplo, si crea un backup en el nodo A e intenta restaurar desde el nodo B, la operación de restauración falla.

Qué hacer

Antes de realizar la operación de restauración desde el nodo B, realice lo siguiente en el nodo B:

1. Añada el repositorio.
2. Sincronice el perfil ejecutando el comando smo profile Sync.
3. Establecer las credenciales del perfil que se utilizará para la operación de restauración ejecutando el comando smo credential set.
4. Actualice el perfil para añadir el nuevo nombre de host y el SID correspondiente ejecutando el comando smo profile update.

Dónde obtener más información

Puede encontrar información sobre las tareas básicas relacionadas con la instalación y el uso de SnapManager.

Documentar	Descripción
Página de descripción de SnapManager	Esta página proporciona información sobre SnapManager, los punteros a la documentación en línea y un enlace a la página de descarga de SnapManager, desde la cual se puede descargar el software.
Guía de configuración DE SAN Data ONTAP para 7-Mode	Este documento está disponible en "mysupport.netapp.com". Se trata de un documento dinámico online que contiene la información más actualizada sobre los requisitos para configurar un sistema en un entorno SAN. Contiene información detallada sobre sistemas de almacenamiento y plataformas de host, problemas de cableado, problemas de switch y configuraciones.
Matriz de compatibilidad de SnapManager y SnapDrive	Este documento está disponible en la sección interoperabilidad de "mysupport.netapp.com/matrix". Se trata de un documento dinámico online que contiene la información más actualizada específica de SnapManager y sus requisitos de plataforma.
Notas de la versión de SnapManager	Este documento incluye SnapManager. También puede descargar una copia desde "mysupport.netapp.com". Contiene información de última hora que necesita para poner la configuración en funcionamiento sin problemas.

Documentación sobre la conexión para host y los kits de soporte de NetApp	"mysupport.netapp.com".
Guía de configuración del sistema	"mysupport.netapp.com".
Guía de gestión de acceso en bloques de Data ONTAP	"mysupport.netapp.com"
Información del sistema operativo y de la base de datos del host	Estos documentos proporcionan información acerca del sistema operativo del host y el software de la base de datos.

Clasificación de mensajes de error

Puede determinar la causa de un error si conoce las clasificaciones de mensajes.

En la siguiente tabla, se proporciona información acerca de los rangos numéricos de los diferentes tipos de mensajes que puede ver con SnapManager:

Grupo	Rango	Uso
ENTORNO ORACLE	1000-1999	Se utiliza para registrar el estado o los problemas con el entorno operativo de SnapManager. Este grupo incluye mensajes sobre los sistemas con los que SnapManager interactúa, por ejemplo, con el host, el sistema de almacenamiento, la base de datos, etc.
BACKUP	2000-2999	Asociados con el proceso de backup de la base de datos.
RESTAURAR	3000-3999	Asociados con el proceso de restauración de bases de datos.
CLONAR	4000-4999	Asociados con el proceso de clonado de base de datos.
PERFIL	5000-5999	Se utiliza para administrar perfiles.
GESTIONE	6000-6999	Se utiliza para gestionar backups.
INTERFAZ DE BASES DE DATOS VIRTUALES	7000-7999	Asociado con la interfaz de base de datos virtual.

INTERFAZ DE ALMACENAMIENTO VIRTUAL	8000-8999	Asociado con la interfaz de almacenamiento virtual.
REPOSITORIO	9000-9999	Asociado con la interfaz del repositorio.
MÉTRICAS	10000-10999	Asociados con el tamaño del backup de base de datos, tiempo transcurrido para realizar el backup, tiempo para restaurar la base de datos, número de veces que se clona una base de datos, etc.
INTERFAZ DE HOST VIRTUAL	11000-11999	Asociado con la interfaz del host virtual. Esta es la interfaz para el sistema operativo del host.
EJECUCIÓN	12000-12999	Asociado al paquete de ejecución, incluidas las llamadas al sistema operativo de desove y procesamiento.
PROCESO	13000-13999	Asociado con el componente de proceso de SnapManager.
SERVICIOS PÚBLICOS	14000-14999	Asociados con las utilidades de SnapManager, el contexto global, etc.
VOLCADO/DIAGNÓSTICO	15000-15999	Asociados con operaciones de volcado o diagnóstico.
AYUDA	16000-16999	Asociado con ayuda.
SERVIDOR	17000-17999	Se utiliza en la administración del servidor SnapManager.
API	18000-18999	Asociado con la API.
AUTOR	20000-20999	Asociado con la autorización de credenciales.

Mensajes de error

Es posible encontrar información sobre los mensajes de error asociados a diferentes operaciones de SnapManager.

Mensajes de error más comunes

En la siguiente tabla se enumeran algunos de los errores más comunes e importantes asociados con SnapManager para Oracle:

Mensaje de error	Explicación	Resolución
SD-10038: El sistema de archivos no se puede escribir.	El proceso de SnapManager no tiene acceso de escritura al sistema de archivos.	Debe asegurarse de que el proceso de SnapManager tenga acceso de escritura al sistema de archivos. Después de corregir esto, es posible que deba tomar otra instantánea.
SMO-05075: No se puede crear el perfil. Debe configurar la relación DP/XDP correctamente o elegir la política de protección correcta según la relación subyacente.	Los volúmenes subyacentes no están en una relación de SnapVault ni de SnapMirror.	Debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.
SMO-05503: Se ha especificado el mismo nombre al perfil. Especifique un nombre diferente para cambiar el nombre del perfil.	Los perfiles con nombres idénticos no pueden existir en un repositorio.	Introduzca un nombre de perfil que no esté en uso.
SMO-05505: No se pueden actualizar los metadatos del conjunto de datos.	Es posible que el conjunto de datos se haya eliminado o no exista.	Antes de actualizar los metadatos del conjunto de datos, compruebe que el conjunto de datos existe mediante la consola de gestión de NetApp.
SMO-05506: No se puede actualizar el perfil porque hay operaciones en ejecución en el perfil. Debe esperar hasta que la operación o operaciones se completen y, a continuación, actualizar el perfil.	El perfil no se puede actualizar cuando hay operaciones de backup, restauración y clonado en curso.	Actualice el perfil una vez completada la operación actual.
SMO-05509: Duración de la retención primaria de archive velog no válida; especifique un valor entero positivo.	La duración de la retención de los backups de registros de archivos no puede ser negativa.	Especifique un valor positivo para la duración de la retención de los backups de registros de archivos.

SMO-07463: Esta restauración de backups requiere que la base de datos esté en el estado requerido. Error al llevar la base de datos al estado requerido.	La base de datos no está en el estado requerido para una operación de backup.	Compruebe que la base de datos esté en estado relevante antes de crear una copia de backup. El estado de la base de datos que se va a restaurar depende del tipo de proceso de restauración que se desee realizar y del tipo de archivos que se incluirán.
SMO-09315: Después de realizar una actualización o una operación de actualización del repositorio, es posible que no se reciba la notificación de resumen para las notificaciones establecidas en la versión anterior, a menos que se actualice la notificación de resumen con los detalles del host de notificación.	Los ajustes de notificación no se configuran para el repositorio después de una actualización gradual.	Después de una actualización gradual, actualice la configuración de notificación de resumen para recibir notificaciones.
SM0-02076: El nombre de la etiqueta no debe contener ningún carácter especial que no sea el guión bajo.	El nombre de la etiqueta contiene caracteres especiales distintos del guión bajo.	El nombre de la etiqueta debe ser único dentro del perfil. El nombre puede contener letras, números, un guión bajo (_) y un guión (-) (pero no puede comenzar con un guión). Asegúrese de que las etiquetas no contengan caracteres especiales excepto el guion bajo.
SMO-06308: Excepción al intentar iniciar la programación: java.lang.NullPointerException	Se configura el nombre de dominio completo (FQDN) del host de perfil en lugar del nombre de host del sistema y no se puede resolver el FQDN del host de perfil.	Asegúrese de usar el nombre de host del sistema y no el FQDN.
Error en ExecuteRestoreSteps: ORACLE-10003: Error al ejecutar SQL "DROP DISKGROUP;control nombre del grupo de discos; INCLUIDO CONTENIDO" contra la base de datos Oracle +ASM1: ORA-15039: diskgroup no eliminados ORA-15027: Uso activo del grupo de discos; "control del nombre del grupo de discos;" impide su desmontaje	La operación para restaurar un backup con archivos de control no puede soltar el grupo de discos de control. Este problema ocurre si hay archivos de control de copia de seguridad obsoletos en el grupo de discos de control.	Identifique los archivos de control de copia de seguridad obsoletos y elimínelos manualmente.

RMAN-06004: Error DE ORACLE de la base de datos del catálogo de recuperación: ORA-01424: Carácter ausente o ilegal después del carácter de escape	La operación de creación de backup no se pudo quitar la copia de backup del catálogo cuando SnapManager está integrada con RMAN.	Compruebe si hay secuencias de comandos externas utilizadas para eliminar las copias de seguridad de RMAN. Ejecute el comando CROSSCHECK BACKUP en RMAN para actualizar el repositorio de RMAN y el comando resync catalog para sincronizar el archivo de control de la base de datos de destino con el catálogo de recuperación.
[DEBUG]: Excepción al eliminar la copia de seguridad. java.lang.IllegalStateException: [Assertion failed] - este estado invariante debe ser true	Se crean múltiples copias de Snapshot para un solo ID de operación.	Eliminar las copias Snapshot manualmente y utilizar scripts para eliminar las entradas del repositorio.
La hora y la hora del sistema que muestra SnapManager en los archivos de registro no coinciden o no están sincronizados.	Java 7 aún no admite un cambio de zona horaria.	Aplique la revisión tzUpdater proporcionada por Oracle.
DISC-00001: No se puede detectar almacenamiento: El siguiente identificador no existe o no es del tipo esperado: Archivo ASM	Los archivos de datos o de control o los redo logs se multiplexan en una base de datos ASM.	Extraiga el multiplexado de Oracle.
ORA-01031: Privilegios insuficientes. Compruebe que el servicio Windows de SnapManager está configurado para ejecutarse como usuario con los privilegios correctos y que el usuario está incluido en el grupo ORA_DBA.	No tiene privilegios suficientes en SnapManager. La cuenta de servicio de SnapManager no forma parte del grupo ORA_DBA.	Haga clic con el botón derecho del ratón en el icono **PC** del escritorio y seleccione **gestionar** para comprobar que la cuenta de usuario del servicio SnapManager forma parte del grupo ORA_DBA. Compruebe los usuarios y grupos locales y asegúrese de que la cuenta forma parte del grupo ORA_DBA. Si el usuario es el administrador local, asegúrese de que el usuario está en el grupo en lugar del administrador del dominio.

0001-SMO-02016: Es posible que haya habido tablas externas en la base de datos de las que no se ha realizado un backup como parte de esta operación de backup (ya que la base de datos no estaba ABIERTA durante esta copia de seguridad ALL_EXTERNAL_LOCATIONS no se pudo consultar para determinar si existen tablas externas o no).	SnapManager no realiza copias de seguridad de tablas externas (por ejemplo, tablas que no están almacenadas en archivos .dbf). Este problema se produce porque la base de datos no estaba abierta durante el backup, SnapManager no puede determinar si se están utilizando tablas externas.	Puede haber tablas externas en la base de datos que no se incluyeron en un backup como parte de esta operación (porque la base de datos no estaba abierta durante el backup).
0002-332 error de administrador: No se ha podido comprobar SD.snapshot.Clone el acceso al volumen "volume_name" del nombre de usuario de usuario en los servidores de Operations Manager "dfm_Server". Motivo: El recurso especificado no es válido. No se puede encontrar su ID en Operations Manager Server "dfm_Server"	No se han configurado los privilegios de acceso adecuados y los roles.	Defina los privilegios de acceso o los roles para los usuarios que intentan ejecutar el comando.
[WARN] FLOW-11011: Operación cancelada [ERROR] FLOW-11008: Error de operación: Error de operación: Espacio de pila Java.	Hay más archivos de registro de archivos en la base de datos que el máximo permitido.	1. Desplácese hasta el directorio de instalación de SnapManager. 2. Abra el archivo Launch-java. 3. Aumente el valor de `java -Xmx160m` Parámetro Java heap space . Por ejemplo, puede modificar el valor del valor predeterminado de 160 m a 200 m. `java -Xmx200m`.
SMO-21019: No se pudo realizar la poda del registro de archivo para el destino: "E:\dest" con el motivo: "ORACLE-00101: Error al ejecutar el comando RMAN: [DELETE NOPROMET ARCHIVELOG 'E:\dest']	La eliminación del registro de archivo falla en uno de los destinos. En este caso, SnapManager continúa depurando los archivos de registro de archivos de los otros destinos. Si algún archivo se elimina manualmente del sistema de archivos activo, RMAN no puede hacer una copia de los archivos de registro de archivos de ese destino.	Conéctese a RMAN desde el host SnapManager. Ejecute el comando CROSSCHECK ARCHIVELOG ALL de RMAN y vuelva a realizar la operación de eliminación en los archivos de registro de archivos.

SMO-13032: No se puede realizar la operación: Archive log Prune. Causa raíz: Excepción de RMAN: ORACLE-00101: Error al ejecutar el comando RMAN.	Los archivos de registro de archivos se eliminan manualmente de los destinos de registro de archivos.	Conéctese a RMAN desde el host SnapManager. Ejecute el comando CROSSCHECK ARCHIVELOG ALL de RMAN y vuelva a realizar la operación de eliminación en los archivos de registro de archivos.
No se puede analizar la salida del shell: (java.util.regex.Matcher[pattern=Command Complete. Region=0,18 lastmatch=]) no coincide (name:backup_script) no se puede analizar la salida del shell: (java.util.regex.Matcher[pattern=Command complete. region=0,25 lastmatch=]) no coincide (description:script backup) No se puede analizar la salida del shell: (java.util.regex.Matcher[pattern=Command Complete. region=0,9 lastmatch=]) no coincide (timeout:0)	Las variables de entorno no se definen correctamente en los scripts previos o posteriores a las tareas.	Compruebe si las secuencias de comandos previas o posteriores a las tareas siguen la estructura del complemento SnapManager estándar. Para obtener información adicional sobre el uso de las variables de entorno en el script, consulte Operaciones en scripts de tareas.
ORA-01450: Se ha superado la longitud máxima de la llave (6398).	Cuando se realiza una actualización de SnapManager 3.2 para Oracle a SnapManager 3.3 para Oracle, la operación de actualización se produce un error con este mensaje de error. Este problema puede ocurrir debido a uno de los siguientes motivos: • El tamaño de bloque del tablespace en el que existe el repositorio es inferior a 8k. • El parámetro nls_length_semántica se establece en char.	Debe asignar los valores a los siguientes parámetros: • block_size=8192 • nls_length=byte Después de modificar los valores de los parámetros, debe reiniciar la base de datos. Para obtener más información, consulte el artículo 2017632 de la base de conocimientos.

Mensajes de error asociados con el proceso de copia de seguridad de la base de datos (serie 2000)

En la siguiente tabla se enumeran los errores comunes asociados al proceso de copia de seguridad de la base de datos:

Mensaje de error	Explicación	Resolución

SMO-02066: No es posible eliminar ni liberar los "registros de datos" del backup de registros de archivo, ya que el backup está asociado a los "registros de datos" del backup de datos.	La copia de seguridad del registro de archivos se realiza junto con la copia de seguridad de los archivos de datos y se intentó eliminar el backup del registro de archivos.	Utilice la opción -force para eliminar o liberar el backup.
SMO-02067: No se puede eliminar ni liberar los "registros de datos" del backup de registros de archivo, ya que el backup está asociado a los "registros de datos" del backup de datos y se encuentra dentro de la duración de retención asignada.	El backup de registros de archivos se asocia con el backup de la base de datos y se encuentra dentro del período de retención, y se intentó eliminar el backup de registros de archivos.	Utilice la opción -force para eliminar o liberar el backup.
SMO-07142: Registros archivados excluidos debido al patrón de exclusión <exclusion>.	Se excluyen algunos archivos de registro de archivos durante la operación de creación de perfiles o creación de copias de seguridad.	No se requiere ninguna acción.
SMO-07155: Los archivos de registro archivados de <count> no existen en el sistema de archivos activo. Estos archivos de registro archivados no se incluirán en la copia de seguridad.	Los archivos de registro de archivos no existen en el sistema de archivos activo durante la operación de creación de perfiles o de creación de backup. Estos archivos de registro archivados no se incluyen en la copia de seguridad.	No se requiere ninguna acción.
SMO-07148: Los archivos de registro archivados no están disponibles.	No se crean archivos de registro de archivos para la base de datos actual durante la operación de creación de perfiles o creación de backups.	No se requiere ninguna acción.
SMO-07150: No se encuentran los archivos de registro archivados.	Faltan todos los archivos de registro de archivos del sistema de archivos o se excluyen durante la operación de creación de perfiles o creación de copia de seguridad.	No se requiere ninguna acción.

SMO-13032: No se puede realizar la operación: Crear un backup. Causa raíz: ORACLE-20001: Error al intentar cambiar el estado A ABIERTO para la instancia de base de datos dfcln1: ORACLE-20004: Esperando poder abrir la base de datos sin la opción RESETLOGS, pero oracle está informando de que la base de datos necesita abrirse con la opción RESETLOGS. Para evitar que se restableciendo inesperadamente los registros, el proceso no continuará. Asegúrese de que la base de datos se puede abrir sin la opción RESETLOGS e inténtelo de nuevo.	Se intenta realizar una copia de seguridad de la base de datos clonada que se creó con la opción -no-resetlogs. La base de datos clonada no es una base de datos completa. Sin embargo, es posible ejecutar operaciones de SnapManager, como la creación de perfiles y backups, etc. con la base de datos clonada, pero se produce un error en las operaciones de SnapManager debido a que la base de datos clonada no está configurada como una base de datos completa.	Recuperar la base de datos clonada o convertir la base de datos a una base de datos de Data Guard en espera.

Mensajes de error asociados con el proceso de restauración (serie 3000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de restauración:

Mensaje de error	Explicación	Resolución
SMO-03031:Restore especifica para restaurar el <variable> de backup, pues los recursos de almacenamiento para el backup ya se han liberado.	Intentó restaurar una copia de seguridad que tiene liberados sus recursos de almacenamiento sin especificar una especificación de restauración.	Especifique una especificación de restauración.
SMO-03032:Restore especificación debe contener asignaciones para los archivos que restaurar, pues los recursos de almacenamiento del backup ya se han liberado. Los archivos que necesitan asignaciones son: <variable> desde instantáneas: <variable>	Intentó restaurar una copia de seguridad que tiene liberados sus recursos de almacenamiento junto con una especificación de restauración que no contiene la asignación de todos los archivos que se van a restaurar.	Corrija el archivo de especificación de restauración de modo que las asignaciones coincidan con los archivos que se van a restaurar.

ORACLE-30028: No se puede volcar el <filename> del archivo de registro. Es posible que el archivo esté ausente/inaccesible/dañado. Este archivo de registro no se utilizará para la recuperación.	Los archivos redo log en línea o los archivos archive log no se pueden utilizar para la recuperación.este error se produce debido a los siguientes motivos: • Los archivos redo log en línea o los archivos archive log mencionados en el mensaje de error no tienen números de cambio suficientes para solicitar la recuperación. Esto ocurre cuando la base de datos está en línea sin ninguna transacción. Los archivos redo log o archive log no tienen ningún número de cambio válido que se pueda aplicar para la recuperación. • El archivo redo log en línea o el archivo archive log mencionado en el mensaje de error no tiene suficientes privilegios de acceso para Oracle. • El archivo redo log en línea o el archivo de registro archivado mencionado en el mensaje de error están dañados y Oracle no puede leerlos. • El archivo redo log en línea o el archivo de registro archivado mencionado en el mensaje de error no se encuentra en la ruta de acceso mencionada.	Si el archivo mencionado en el mensaje de error es un archivo de registro archivado y si ha proporcionado manualmente para la recuperación, asegúrese de que el archivo tiene permisos de acceso completo a Oracle.incluso si el archivo tiene permisos completos, y el mensaje continúa, el archivo de registro de archivo no tiene ningún número de cambio que se aplicará para la recuperación, y este mensaje puede ignorarse.

Mensajes de error asociados con el proceso de clonación (serie 4000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de clonación:

Mensaje de error	Explicación	Resolución
SMO-04133: El destino de volcado no debe existir	Se está utilizando SnapManager para crear nuevos clones; sin embargo, los destinos de volcado que usará el nuevo clon ya existen. SnapManager no puede crear un clon si existen destinos de volcado.	Quite o cambie el nombre de los destinos de volcado antiguos antes de crear un clon.

SMO-13032: No se puede realizar la operación: Clone Create. Causa raíz: ORACLE-00001: Error al ejecutar SQL: [ALTER DATABASE OPEN RESETLOGS;]. El comando devolvió: ORA-38856: No se puede marcar la instancia UNNAMED_INSTANCE_2 (redo thread 2) como habilitada.	Se produce un error en la creación del clon cuando se crea desde la base de datos en espera con la siguiente configuración: • El modo de espera se crea mediante RMAN para realizar una copia de seguridad de los archivos de datos.	Añada el parámetro _no_recovery_through_resetlogs= TRUE en el archivo de especificación del clon antes de crearlo. Consulte la documentación de Oracle (ID 334899.1) para obtener información adicional. Asegúrese de tener el nombre de usuario y la contraseña de Oracle metalink.
	No ha especificado un valor para un parámetro en el archivo de especificación del clon.	Debe proporcionar un valor para el parámetro o eliminar ese parámetro si no es necesario en el archivo de especificación del clon.

Mensajes de error asociados con el proceso de gestión de perfiles (serie 5000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de clonación:

Mensaje de error	Explicación	Resolución
SMO-20600: No se ha encontrado el perfil "profile1" en el repositorio "repo_name". Ejecute "Profile SYNC" para actualizar las asignaciones de perfil a repositorio.	La operación de volcado no se puede realizar cuando se produce un error al crear el perfil.	Utilice el sistema de volcado.

Mensajes de error asociados con la liberación de recursos de backup (series de backups 6000)

En la siguiente tabla se muestran los errores comunes asociados con las tareas de backup:

Mensaje de error	Explicación	Resolución
SMO-06030: No se puede eliminar el backup porque está en uso: <variable>	Se intentó realizar la operación de backup libre con comandos, cuando el backup está montado o tiene clones, o bien se Marca para que se conserve de forma ilimitada.	Desmonte el backup o cambie la política de retención ilimitada. Si hay clones, elimínelos.
SMO-06045: No se puede liberar el <variable> de backup porque los recursos de almacenamiento para el backup ya se han liberado	Se intentó realizar la operación de backup libre con comandos, cuando ya se ha liberado el backup.	No se puede liberar la copia de seguridad si ya se ha liberado.

SMO-06047: Solo se pueden liberar los backups realizados correctamente. El estado de <ID> de backup es <status>.	Se intentó realizar la operación de backup libre con comandos, cuando el estado del backup no es correcto.	Vuelva a intentarlo después de realizar el backup correctamente.
SMO-13082: No es posible realizar una operación de <variable> en la <ID> de backup porque se han liberado los recursos de almacenamiento para el backup.	Con comandos, se intentó montar un backup con los recursos de almacenamiento liberados.	No es posible montar, clonar o verificar un backup que tenga liberados sus recursos de almacenamiento.

Mensajes de error asociados con el proceso de actualización gradual (serie 9000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de actualización gradual:

Mensaje de error	Explicación	Resolución
SMO-09234: Los hosts siguientes no existen en el almacén antiguo. <hostnames>.	Intentó realizar una actualización gradual de un host, que no existe en la versión de repositorio anterior.	Compruebe si el host existe en el repositorio anterior con el comando Repository show-Repository de la versión anterior de la interfaz de línea de comandos de SnapManager.
SMO-09255: Los hosts siguientes no existen en el nuevo almacén. <hostnames>.	Intentó realizar la reversión de un host, que no existe en la versión del nuevo repositorio.	Compruebe si el host existe en el nuevo repositorio con el comando Repository show-Repository de la versión posterior de la CLI de SnapManager.
SMO-09256:Rollback no se admite, ya que existe un nuevo perfil <profilenames>.for the hosts <hostnames> especificados.	Intentó revertir un host que contiene nuevos perfiles existentes en el repositorio. Sin embargo, estos perfiles no existían en el host de la versión anterior de SnapManager.	Elimine nuevos perfiles en la versión posterior o actualizada de SnapManager antes de la reversión.
SMO-09257:Rollback no se admite, ya que los backups <backupid> están montados en los nuevos hosts.	Intentó revertir una versión posterior del host SnapManager que tiene backups montados. Estos backups no se montan en la versión anterior del host SnapManager.	Desmonte los backups en la versión posterior del host SnapManager y, a continuación, realice la reversión.
SMO-09258: No se admite la reversión, ya que los backups <backupid> se desasocian de los nuevos hosts.	Ha intentado revertir una versión posterior del host SnapManager que tiene backups que se están desdesmontan.	Monte los backups en la versión posterior del host SnapManager y, a continuación, ejecute la reversión.

SMO-09298: No se puede actualizar este almacén porque ya tiene otros hosts en la versión superior. En su lugar, ejecute rollingupgrade para todos los hosts.	Realizó una actualización gradual en un solo host y, después, actualizó el repositorio para ese host.	Realice una actualización gradual en todos los hosts.
SMO-09297: Se ha producido un error al habilitar las restricciones. El repositorio puede estar en estado incoherente. Se recomienda restaurar el backup del repositorio que haya tomado antes de la operación actual.	Se intentó realizar una operación de reversión o actualización sucesiva si la base de datos del repositorio queda en estado incoherente.	Restaurar el repositorio del que se ha hecho backup anteriormente.

Ejecución de operaciones (serie 12,000)

En la siguiente tabla se muestran los errores comunes asociados a las operaciones:

Mensaje de error	Explicación	Resolución
SMO-12347 [ERROR]: El servidor SnapManager no se ejecuta en la <host> del host y en la <port> de puertos. Ejecute este comando en un host que ejecuta el servidor SnapManager.	Al configurar el perfil, debe introducir información sobre el host y el puerto. Sin embargo, SnapManager no puede realizar estas operaciones porque el servidor SnapManager no está en ejecución en el host y el puerto especificados.	Introduzca el comando en un host que ejecuta el servidor SnapManager. Puede comprobar el puerto con el comando lsnrctl status y ver el puerto en el que se ejecuta la base de datos. Si es necesario, cambie el puerto del comando backup.

Ejecución de componentes de proceso (serie 13,000)

En la siguiente tabla se muestran los errores comunes asociados con el componente de proceso de SnapManager:

Mensaje de error	Explicación	Resolución
SMO-13083: El patrón de Snapname con el valor "x" contiene caracteres que no son letras, números, guion bajo, guion y llaves.	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha incluido caracteres especiales que no están permitidos.	Quite caracteres especiales que no sean letras, números, guion bajo, guion y corchetes.
SMO-13084: El patrón de Snapname con el valor "x" no contiene el mismo número de llaves izquierda o derecha.	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, las llaves izquierda y derecha no coinciden.	Introduzca los corchetes de apertura y cierre coincidentes en el patrón de Snapname.

SMO-13085: El patrón de Snapname con el valor "x" contiene un nombre de variable no válido de "y".	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha incluido una variable que no está permitida.	Elimine la variable ofensor. Para ver una lista de variables aceptables, consulte Nomenclatura de copias Snapshot.
El patrón de Snapname de SMO-13086 con el valor "x" debe contener la variable "smid".	Al crear un perfil, ha personalizado el patrón Snapname; sin embargo, ha omitido la variable smid necesaria.	Inserte la variable smid necesaria.

Mensajes de error asociados con utilidades de SnapManager (serie 14,000)

En la siguiente tabla se muestran los errores comunes asociados con las utilidades de SnapManager:

Mensaje de error	Explicación	Resolución
SMO-14501: El ID de correo no puede estar vacío.	No ha introducido la dirección de correo electrónico.	Introduzca una dirección de correo electrónico válida.
SMO-14502: El asunto del correo no puede estar vacío.	No ha introducido el asunto del correo electrónico.	Introduzca el asunto del correo electrónico que corresponda.
SMO-14506: El campo del servidor de correo no puede estar vacío.	No se introdujo el nombre de host ni la dirección IP del servidor de correo electrónico.	Introduzca el nombre de host o la dirección IP del servidor de correo válido.
SMO-14507: El campo Puerto de correo no puede estar vacío.	No ha introducido el número de puerto de correo electrónico.	Introduzca el número de puerto del servidor de correo electrónico.
SMO-14508: Del ID de correo no puede estar en blanco.	No ha introducido la dirección de correo electrónico del remitente.	Introduzca una dirección de correo electrónico del remitente válida.
SMO-14509: El nombre de usuario no puede estar vacío.	Habilitó la autenticación y no proporcionó el nombre de usuario.	Introduzca el nombre de usuario de autenticación por correo electrónico.
SMO-14510: La contraseña no puede estar vacía. Introduzca la contraseña.	Habilitó la autenticación y no proporcionó la contraseña.	Introduzca la contraseña de autenticación por correo electrónico.
SMO-14550: Estado del correo electrónico: <success/failure>.	El número de puerto, el servidor de correo o la dirección de correo electrónico del receptor no son válidos.	Proporcione los valores adecuados durante la configuración del correo electrónico.

SMO-14559: Error al enviar una notificación de correo electrónico: <error>.	Esto podría deberse a un número de puerto no válido, a un servidor de correo no válido o a una dirección de correo del destinatario no válida.	Proporcione los valores adecuados durante la configuración del correo electrónico.
SMO-14560: Error de notificación: La configuración de la notificación no está disponible.	Error en el envío de notificaciones porque la configuración de notificación no está disponible.	Agregar configuración de notificación.
SMO-14565: Formato de hora no válido. Introduzca el formato de hora en HH:mm.	Introdujo la hora en un formato incorrecto.	Introduzca la hora en el formato: hh:mm.
SMO-14566: Valor de fecha no válido. El rango de fechas válido es 1-31.	La fecha configurada es incorrecta.	La fecha debe estar entre 1 y 31.
SMO-14567: Valor del día no válido. El rango de días válido es de 1 a 7.	El día configurado es incorrecto.	Introduzca el intervalo de días del 1 al 7.
SMO-14569: El servidor no pudo iniciar la programación de notificaciones de resumen.	El servidor SnapManager se cerró por motivos desconocidos.	Inicie el servidor SnapManager.
SMO-14570: Notificación resumida no disponible.	No ha configurado la notificación de resumen.	Configure la notificación de resumen.
SMO-14571: No se pueden habilitar las notificaciones de perfil y de resumen.	Ha seleccionado las opciones de notificación de perfil y resumen.	Habilite la notificación de perfil o la notificación de resumen.
SMO-14572: Proporcione un éxito o una opción de fallo para las notificaciones.	No ha habilitado las opciones de éxito o fallo.	Debe seleccionar Success o Failure Option o both.

Información relacionada

Nomenclatura de copias Snapshot

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

"Aviso sobre SnapManager para Oracle"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.