# Documentación sobre el software SnapCenter

SnapCenter Software 4.5

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-45/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

# Tabla de contenidos


Documentación sobre el software SnapCenter . . . 1
Notas de la versión . . . 2
Conceptos . . . 3
- Información general de SnapCenter . . . 3
  - Arquitectura SnapCenter . . . 4
  - Componentes de SnapCenter . . . 5
  - Servidor SnapCenter . . . 6
  - Plugins de SnapCenter . . . 6
  - Repositorio de SnapCenter . . . 9
- Funciones de seguridad . . . 9
  - Descripción general del certificado CA . . . 10
- Control de acceso basado en roles (RBAC) de SnapCenter . . . 10
  - Tipos de RBAC . . . 10
  - Permisos y roles de RBAC . . . 12
  - Roles y permisos predefinidos de SnapCenter . . . 13
- Recursos, grupos de recursos y políticas . . . 17
- Scripts previos y posteriores . . . 18
  - Tipos de scripts compatibles . . . 19
  - Ruta del script . . . 19
  - Dónde especificar scripts . . . 19
  - Tiempo de espera de scripts . . . 19
  - Salida de script . . . 20
- Automatización de SnapCenter mediante API de REST . . . 20

Instalación del servidor SnapCenter . . . 21
- Flujo de trabajo de instalación . . . 21
- Prepare la instalación del servidor SnapCenter . . . 21
  - Requisitos de dominio y grupo de trabajo . . . 21
  - Requisitos de espacio y de tamaño . . . 22
  - Requisitos del host SAN . . . 23
  - Sistemas de almacenamiento y aplicaciones compatibles . . . 23
  - Exploradores compatibles . . . 24
  - Requisitos de conexión y puerto . . . 24
  - Licencias SnapCenter . . . 28
  - Métodos de autenticación para las credenciales . . . 31
  - Conexiones de almacenamiento y credenciales . . . 32
- Instale el servidor SnapCenter . . . 33
- Inicie sesión en SnapCenter . . . 34
  - Modifique el tiempo de espera de sesión de interfaz gráfica de usuario predeterminada de SnapCenter . . . 36
  - Proteja el servidor web de SnapCenter mediante la desactivación de SSL 3.0 . . . 36
- Configurar certificado de CA . . . 36
  - Genere un archivo CSR de certificado de CA . . . 36
  - Importar certificados de CA . . . 37

Obtenga la huella digital del certificado de CA . . . 38
Configure el certificado de CA con servicios de plugins de host de Windows . . . 38
Configurar el certificado de CA con el sitio SnapCenter . . . 39
Habilite los certificados de CA para SnapCenter . . . 40
Registrar dominios de Active Directory que no son de confianza . . . 40
Configuración de la alta disponibilidad . . . 41
Configurar servidores SnapCenter para alta disponibilidad mediante F5 . . . 41
Configure el balanceador de carga de red de Microsoft manualmente . . . 43
Cambie de NLB a F5 para ofrecer alta disponibilidad . . . 43
Alta disponibilidad del repositorio MySQL de SnapCenter . . . 43
Exportar certificados SnapCenter . . . 44
Configurar el control de acceso basado en roles (RBAC) . . . 45
Añada un usuario o grupo y asigne roles y activos . . . 45
Crear un rol . . . 48
Añadir un rol de RBAC de ONTAP mediante comandos de inicio de sesión de seguridad . . . 48
Cree roles de SVM con privilegios mínimos . . . 50
Cree roles de clúster ONTAP con privilegios mínimos . . . 54
Configure los grupos de aplicaciones de IIS para habilitar los permisos de lectura de Active Directory . . . 60
Añadir sistemas de almacenamiento . . . 61
Añada licencias estándar basadas en controladora de SnapCenter . . . 64
Requisitos previos para añadir una licencia basada en controladora . . . 64
Añada una licencia basada en controladora . . . 68
Añada licencias basadas en capacidad estándar de SnapCenter . . . 69
Requisitos previos para añadir licencias basadas en capacidad . . . 70
Añada una licencia basada en capacidad . . . 72
Aprovisione su sistema de almacenamiento . . . 74
Aprovisionar almacenamiento en hosts Windows . . . 74
Aprovisione almacenamiento en entornos VMware . . . 89
Configure las conexiones MySQL protegidas con SnapCenter Server . . . 92
Configure conexiones MySQL protegidas para configuraciones de servidor SnapCenter independientes . . . 92
Configure conexiones MySQL protegidas para configuraciones de alta disponibilidad . . . 94
Funciones habilitadas en su host de Windows durante la instalación . . . 98
Proteger bases de datos de Microsoft SQL Server . . . 102
Plugin de SnapCenter para Microsoft SQL Server . . . 102
Información general sobre el plugin de SnapCenter para Microsoft SQL Server . . . 102
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft SQL Server . . . 102
Funciones del plugin de SnapCenter para Microsoft SQL Server . . . 103
Compatibilidad con asignación de LUN asimétrica en clústeres de Windows . . . 104
Tipos de almacenamiento compatibles con los plugins de SnapCenter para Microsoft Windows y Microsoft SQL Server . . . 105
Recomendaciones sobre distribución de almacenamiento para el plugin de SnapCenter para Microsoft SQL Server . . . 108
Privilegios mínimos de ONTAP requeridos para el plugin de SQL . . . 110
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el

plugin para SQL Server . . . 114
Estrategia de backup para recursos de SQL Server . . . 115
Estrategia de restauración para SQL Server . . . 119
Defina una estrategia de clonación para SQL Server . . . 123
Inicio rápido de instalar el plugin de SnapCenter para SQL Server . . . 124
Preparación de la instalación . . . 124
Instale el servidor SnapCenter . . . 127
Instale el plugin para Microsoft SQL Server . . . 128
Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server . . . 129
Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft SQL Server . . . 129
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft SQL Server . . . 130
Configure credenciales para el paquete de plugins de SnapCenter para Windows . . . 131
Configure las credenciales para un recurso individual de SQL Server . . . 132
Configurar GMSA en Windows Server 2012 o posterior . . . 135
Instale el plugin de SnapCenter para Microsoft SQL Server . . . 136
Configurar certificado de CA . . . 142
Importe los backups archivados de SnapManager para Microsoft SQL Server a SnapCenter . . . 146
Instale el plugin de SnapCenter para VMware vSphere . . . 147
Implemente el certificado de CA . . . 148
Configure el archivo CRL . . . 148
Prepárese para la protección de datos . . . 148
Requisitos previos para utilizar el plugin de SnapCenter para Microsoft SQL Server . . . 148
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger SQL Server . . . 149
Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad . . . 150
Flujo de trabajo de backup . . . 150
Determine si hay recursos disponibles para backup . . . 151
Migrar recursos al sistema de almacenamiento de NetApp . . . 153
Crear políticas de backup para bases de datos de SQL Server . . . 155
Crear grupos de recursos y asociar políticas para SQL Server . . . 162
Requisitos para realizar backups de recursos de SQL . . . 165
Realice backups de recursos de SQL . . . 166
Realizar un backup de grupos de recursos de SQL Server . . . 169
Supervisar las operaciones de backup . . . 170
Cancelar las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server . . . 171
Consulte los backups y los clones de SQL Server en la página Topology . . . 172
Restaure recursos de SQL Server . . . 173
Restaure el flujo de trabajo . . . 173
Requisitos para restaurar una base de datos . . . 174
Restaurar backups de base de datos de SQL Server . . . 175
Restaurar una base de datos de SQL Server a partir de almacenamiento secundario . . . 179
Propagación de bases de datos de grupos de disponibilidad . . . 180
Supervisar operaciones de restauración de recursos de SQL . . . 180
Cancelar las operaciones de restauración de recursos de SQL . . . 181
Clone recursos de bases de datos de SQL Server . . . 182
Flujo de trabajo de clonado . . . 182

Clonar a partir de un backup de base de datos de SQL Server . . . 183
Ejecute el ciclo de vida del clon . . . 186
Supervisar operaciones de clonado de bases de datos de SQL . . . 188
Cancelar las operaciones de clonado de recursos SQL . . . 189
Proteger las bases de datos SAP HANA . . . 190
Plugin de SnapCenter para base de datos SAP HANA . . . 190
Información general sobre el plugin de SnapCenter para bases de datos de SAP HANA . . . 190
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para base de datos SAP HANA . . . 190
Funciones del plugin de SnapCenter para base de datos SAP HANA . . . 190
Tipos de almacenamiento compatibles con el plugin de SnapCenter para base de datos SAP HANA . . . 191
Privilegios mínimos requeridos de ONTAP . . . 192
Preparar los sistemas de almacenamiento para la replicación SnapMirror y SnapVault para las bases de datos SAP HANA . . . 196
Estrategia de backup para las bases de datos SAP HANA . . . 197
Estrategia de restauración y recuperación para bases de datos SAP HANA . . . 200
Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA . . . 203
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA . . . 203
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA . . . 203
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 204
Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA . . . 205
Configurar GMSA en Windows Server 2012 o posterior . . . 208
Instale el plugin de SnapCenter para base de datos SAP HANA . . . 209
Configurar certificado de CA . . . 215
Instale el plugin de SnapCenter para VMware vSphere . . . 223
Implemente el certificado de CA . . . 223
Configure el archivo CRL . . . 223
Prepárese para la protección de datos . . . 223
Requisitos previos para usar el plugin de SnapCenter para base de datos SAP HANA . . . 223
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger bases de datos SAP HANA . . . 224
Realice un backup de los recursos de SAP HANA . . . 225
Realice un backup de los recursos de SAP HANA . . . 225
Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA . . . 226
Descubra recursos y prepare contenedores de bases de datos multitenant para la protección de datos . . . 227
Añada recursos manualmente al host del plugin . . . 230
Crear políticas de backup para bases de datos SAP HANA . . . 231
Crear grupos de recursos y añadir políticas . . . 235
Realice un backup de las bases de datos SAP HANA . . . 238
Realice un backup de los grupos de recursos . . . 241
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos SAP HANA . . . 242
Realizar un backup de bases de datos mediante cmdlets de PowerShell . . . 244

Supervisar las operaciones de backup . . . 247
Consulte los backups y los clones de la base de datos SAP HANA en la página Topology . . . 249
Restaure bases de datos de SAP HANA . . . 250
Restaure el flujo de trabajo . . . 250
Restaurar y recuperar un backup de recurso añadido manualmente . . . 250
Restaurar y recuperar un backup de base de datos detectado automáticamente . . . 252
Restaurar una base de datos SAP HANA mediante cmdlets de PowerShell . . . 256
Supervisar las operaciones de restauración de bases de datos SAP HANA . . . 258
Clonar backups de recursos SAP HANA . . . 259
Flujo de trabajo de clonado . . . 259
Clonar un backup de base de datos SAP HANA . . . 260
Clonar backups de la base de datos SAP HANA mediante cmdlets de PowerShell . . . 262
Supervise las operaciones de clonado de base de datos SAP HANA . . . 263
Divida un clon . . . 264
Elimine o divida los clones de las bases de datos SAP HANA después de actualizar SnapCenter . . . 265
Proteger bases de datos de Oracle . . . 267
Información general del plugin de SnapCenter para base de datos de Oracle . . . 267
Qué puede hacer con el plugin para base de datos de Oracle . . . 267
Funciones del plugin para base de datos de Oracle . . . 267
Tipos de almacenamiento compatibles con el plugin para bases de datos de Oracle . . . 269
Privilegios mínimos requeridos de ONTAP para el plugin para Oracle . . . 270
Instale el plugin de SnapCenter para base de datos de Oracle . . . 273
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos de Oracle . . . 273
Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux o AIX . . . 273
Añada hosts e instale el paquete de plugins para Linux o AIX mediante la interfaz gráfica de usuario . . . 282
Configure el servicio de cargador de plugins de SnapCenter . . . 289
Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux . . . 292
Habilite certificados de CA para plugins . . . 295
Importe datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter . . . 296
Instale el plugin de SnapCenter para VMware vSphere . . . 302
Implemente el certificado de CA . . . 302
Configure el archivo CRL . . . 302
Preparar la protección de bases de datos de Oracle . . . 302
Realice backups de bases de datos de Oracle . . . 304
Flujo de trabajo de backup . . . 304
Definir una estrategia de backup para bases de datos de Oracle . . . 305
Determinar si las bases de datos de Oracle están disponibles para backup . . . 312
Crear políticas de backup para bases de datos de Oracle . . . 314
Crear grupos de recursos y vincular políticas para bases de datos de Oracle . . . 319
Requisitos para realizar backups de una base de datos de Oracle . . . 321
Realice backup de recursos de Oracle . . . 322
Realice backups de grupos de recursos de bases de datos de Oracle . . . 325
Backups de bases de datos de Oracle con comandos de UNIX . . . 326
Supervisar las operaciones de backup de bases de datos de Oracle . . . 327

Cancelar las operaciones de backup de las bases de datos de Oracle . . . 328
Consulte los backups y los clones de las bases de datos de Oracle en la página Topology . . . 329
Montar y desmontar backups de bases de datos . . . 331
Montar un backup de base de datos . . . 331
Desmontar un backup de base de datos . . . 333
Restaurar y recuperar bases de datos de Oracle . . . 333
Restaure el flujo de trabajo . . . 333
Definir una estrategia de restauración y recuperación para bases de datos de Oracle . . . 334
Requisitos para restaurar una base de datos de Oracle . . . 339
Restaurar base de datos de Oracle . . . 339
Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico . . . 344
Restaure y recupere una base de datos conectable mediante la recuperación de un momento específico . . . 346
Restaure y recupere bases de datos de Oracle con comandos de UNIX . . . 348
Supervisar las operaciones de restauración de bases de datos de Oracle . . . 349
Cancelar operaciones de restauración de bases de datos de Oracle . . . 350
Clone la base de datos de Oracle . . . 350
Flujo de trabajo de clonado . . . 351
Defina una estrategia de clonado para bases de datos de Oracle . . . 351
Requisitos para clonar una base de datos de Oracle . . . 352
Clonar el backup de una base de datos de Oracle . . . 354
Clonar una base de datos conectable . . . 362
Clonar backups de bases de datos de Oracle con comandos UNIX . . . 367
Divida el clon de una base de datos de Oracle . . . 367
Clon dividido de una base de datos conectable . . . 368
Supervise las operaciones de clonado de las bases de datos de Oracle . . . 369
Actualizar un clon . . . 370
Eliminar el clon de una base de datos conectables . . . 371
Protección de sistemas de archivos Windows . . . 372
Conceptos del plugin de SnapCenter para Microsoft Windows . . . 372
Información general sobre el plugin de SnapCenter para Microsoft Windows . . . 372
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft Windows . . . 372
Funciones del plugin de SnapCenter para Windows . . . 372
Cómo hace SnapCenter para realizar backup de sistemas de archivos Windows . . . 373
Tipos de almacenamiento compatibles con los plugins de SnapCenter para Microsoft Windows . . . 374
Privilegios mínimos de ONTAP requeridos para el plugin de Windows . . . 376
Preparar los sistemas de almacenamiento para la replicación con SnapMirror y SnapVault . . . 380
Defina una estrategia de backup para sistemas de archivos de Windows . . . 381
Orígenes y destinos de clones para sistemas de archivos Windows . . . 383
Instale el plugin de SnapCenter para Microsoft Windows . . . 383
Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Windows . . . 383
Requisitos de instalación del plugin de SnapCenter para Microsoft Windows . . . 383
Configurar GMSA en Windows Server 2012 o posterior . . . 388
Añada hosts e instale el plugin de SnapCenter para Microsoft Windows . . . 390

Instale el plugin de SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell . . . 393
Instale el plugin de SnapCenter para Microsoft Windows silenciosamente desde la línea de comandos 393
Supervise el estado de instalación del paquete de plugins de SnapCenter . . . 395
Configure el certificado de CA . . . 396
Instale el plugin de SnapCenter para VMware vSphere . . . 399
Implemente el certificado de CA . . . 399
Configure el archivo CRL . . . 399
Realizar backup de sistemas de archivos Windows . . . 399
Realizar backup de sistemas de archivos Windows . . . 399
Determinar la disponibilidad de recursos para los sistemas de archivos Windows . . . 400
Crear políticas de backup para sistemas de archivos Windows . . . 401
Crear grupos de recursos para sistemas de archivos Windows . . . 403
Realice el backup de un solo recurso bajo demanda para sistemas de archivos Windows . . . 406
Realizar un backup de grupos de recursos para sistemas de archivos Windows . . . 408
Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell . . . 409
Realizar backup de recursos con cmdlets de PowerShell . . . 410
Supervisar las operaciones de backup . . . 412
Cancele las operaciones de backup . . . 413
Consulte los backups y los clones relacionados en la página Topology . . . 414
Quitar los backups con el cmdlet de PowerShell . . . 416
Borre el número de backup secundario con cmdlets de PowerShell . . . 416
Restaurar sistemas de archivos Windows . . . 417
Restaurar backups de sistemas de archivos Windows . . . 417
Restaurar recursos mediante los cmdlets de PowerShell . . . 418
Supervisar operaciones de restauración . . . 421
Cancele las operaciones de restauración . . . 422
Clonar sistemas de archivos Windows . . . 423
Clonar desde un backup de sistema de archivos Windows . . . 423
Clonar backups mediante cmdlets de PowerShell . . . 424
Supervise las operaciones de clonación . . . 428
Cancele las operaciones de clonado . . . 429
Divida un clon . . . 430
Proteger las bases de datos de Microsoft Exchange Server . . . 432
Conceptos del plugin de SnapCenter para Microsoft Exchange Server . . . 432
Información general sobre el plugin de SnapCenter para Microsoft Exchange Server . . . 432
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft Exchange Server . . . 432
Tipos de almacenamiento compatibles con el plugin de SnapCenter para Microsoft Windows y Microsoft Exchange Server . . . 433
Privilegios mínimos requeridos de ONTAP . . . 434
Preparar los sistemas de almacenamiento para la replicación con SnapMirror y SnapVault . . . 438
Defina una estrategia de backup para recursos de servidor de Exchange . . . 439
Definir una estrategia de restauración para bases de datos de Exchange . . . 442
Instale el plugin de SnapCenter para Microsoft Exchange Server . . . 443

Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Exchange Server . . . 443
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft Exchange Server . . . 443
Configure credenciales para el plugin de SnapCenter para Windows . . . 447
Configurar GMSA en Windows Server 2012 o posterior . . . 448
Añada hosts e instale el plugin para Exchange . . . 450
Instale el plugin para Exchange desde el host del servidor de SnapCenter mediante cmdlets de PowerShell . . . 453
Instale el plugin de SnapCenter para Exchange silenciosamente desde la línea de comandos . . . 454
Supervise el estado de instalación del paquete de plugins de SnapCenter . . . 456
Configurar certificado de CA . . . 456
Configure SnapManager 7.x para Exchange y SnapCenter para que coexistan . . . 460
Instale el plugin de SnapCenter para VMware vSphere . . . 461
Implemente el certificado de CA . . . 461
Configure el archivo CRL . . . 462
Prepárese para la protección de datos . . . 462
Requisitos previos para usar el plugin de SnapCenter para Microsoft Exchange Server . . . 462
Uso de recursos, grupos de recursos y políticas para proteger un servidor de Exchange . . . 463
Realice backup de recursos de Exchange . . . 464
Flujo de trabajo de backup . . . 464
Verificación de la base de datos y el backup de Exchange . . . 465
Determine si hay recursos de Exchange disponibles para backup . . . 465
Crear políticas de backup para bases de datos de Exchange Server . . . 467
Crear grupos de recursos y añadir políticas para Exchange Server . . . 473
Realizar backup de bases de datos de Exchange . . . 476
Realizar backup de grupos de recursos de Exchange . . . 478
Cree una conexión de sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para Exchange Server . . . 479
Realizar backup de recursos de Exchange con cmdlets de PowerShell . . . 480
Supervisar las operaciones de backup . . . 483
Cancelar las operaciones de backup de la base de datos de Exchange . . . 484
Quitar los backups de Exchange mediante el cmdlet de PowerShell . . . 485
Consulte los backups de Exchange en la página Topology . . . 486
Restaurar recursos de Exchange . . . 487
Restaure el flujo de trabajo . . . 487
Requisitos para restaurar una base de datos de Exchange . . . 487
Restaurar bases de datos de Exchange . . . 488
Recuperación granular de correos y buzones de correo . . . 490
Restaurar una base de datos de servidor de Exchange desde un almacenamiento secundario . . . 490
Restaurar recursos de Exchange mediante cmdlets de PowerShell . . . 491
Propagación de una réplica pasiva del nodo de Exchange . . . 493
Repropagación de una réplica mediante cmdlets de PowerShell para base de datos de Exchange . . . 494
Supervisar operaciones de restauración . . . 494
Cancelar las operaciones de restauración para base de datos de Exchange . . . 495
Proteger aplicaciones personalizadas . . . 497

Plugins personalizados de SnapCenter . . . 497
Información general sobre los plugins personalizados de SnapCenter . . . 497
Tareas que pueden llevarse a cabo con los plugins personalizados de SnapCenter . . . 497
Funciones de los plugins personalizados de SnapCenter . . . 497
Tipos de almacenamiento compatibles con los plugins personalizados de SnapCenter . . . 498
Privilegios mínimos de ONTAP requeridos para el plugin personalizado . . . 499
Prepare los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para los plugins personalizados . . . 503
Defina una estrategia de backup . . . 504
Estrategia de backup para plugins personalizados . . . 504
Tipos de estrategias de restauración compatibles con los recursos de SAP HANA añadidos manualmente . . . 505
Desarrolle un complemento para la aplicación . . . 506
Descripción general . . . 506
Desarrollo basado en PERL . . . 508
Estilo NATIVO . . . 517
Estilo Java . . . 520
Plugin personalizado en SnapCenter . . . 528
Prepare la instalación de los plugins personalizados de SnapCenter . . . 532
Flujo de trabajo de instalación de plugins personalizados de SnapCenter . . . 532
Requisitos previos para añadir hosts e instalar plugins personalizados de SnapCenter . . . 533
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 534
Configure credenciales para los plugins personalizados de SnapCenter . . . 535
Configurar GMSA en Windows Server 2012 o posterior . . . 538
Instale los plugins personalizados de SnapCenter . . . 539
Configurar certificado de CA . . . 546
Prepárese para la protección de datos . . . 554
Requisitos previos para usar los plugins personalizados de SnapCenter . . . 554
Cómo se usan los recursos, los grupos de recursos y las políticas para proteger los recursos de los plugins personalizados . . . 554
Realice backup de recursos de plugins personalizados . . . 555
Realice backup de recursos de plugins personalizados . . . 555
Añada recursos a los plugins personalizados de SnapCenter . . . 556
Crear políticas para recursos de plugins personalizados . . . 559
Crear grupos de recursos y añadir políticas . . . 562
Realice backup de recursos de plugins individuales . . . 566
Realice un backup de grupos de recursos de plugins personalizados . . . 569
Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell . . . 569
Realizar backup de recursos con cmdlets de PowerShell . . . 571
Supervisar las operaciones de backup de los recursos de plugins personalizados . . . 573
Cancelar las operaciones de backup para plugins personalizados . . . 573
Consulte los clones y backups relacionados con los recursos de plugins personalizados en la página Topology . . . 574
Restaure recursos de plugins personalizados . . . 576

Restaure recursos de plugins personalizados . . . 576
Restaurar un backup de recursos . . . 576
Supervisar las operaciones de restauración de recursos de plugins personalizados . . . 578
Clonar backups de recursos de plugins personalizados . . . 579
Clonar backups de recursos de plugins personalizados . . . 579
Clonar desde un backup . . . 580
Clonar backups mediante cmdlets de PowerShell . . . 582
Supervisar las operaciones de clonado de recursos de plugins personalizados . . . 585
Gestione SnapCenter Server y los plugins . . . 587
Consola de visualización . . . 587
Información general de la consola . . . 587
Cómo ver información en el panel . . . 591
Solicite informes de estado de trabajos desde la consola . . . 592
Solicite informes sobre el estado de protección desde el panel de control . . . 592
Gestione RBAC . . . 593
Modificar un rol . . . 593
Modificar usuarios y grupos . . . 594
Gestionar hosts . . . 594
Actualizar la información de la máquina virtual . . . 595
Modifique los hosts de plugins . . . 596
Inicie o reinicie servicios de plugin . . . 597
Suspender programaciones del mantenimiento del host . . . 597
Operaciones admitidas en la página Resources . . . 598
Gestionar políticas . . . 599
Modificar políticas . . . 599
Desvincular políticas . . . 600
Eliminar políticas . . . 600
Gestione grupos de recursos . . . 601
Detenga y reanude operaciones en grupos de recursos . . . 601
Eliminar grupos de recursos . . . 602
Gestionar backups . . . 602
Cambiar el nombre de los backups . . . 602
Eliminar backups . . . 603
Eliminar clones . . . 603
Supervisar trabajos, programaciones, eventos y registros . . . 604
Supervisar trabajos . . . 604
Supervisar programaciones . . . 605
Supervisar eventos . . . 605
Supervisar registros . . . 605
Quite los trabajos y los registros de SnapCenter . . . 606
Información general sobre las funcionalidades de generación de informes de SnapCenter . . . 607
Acceder a informes . . . 609
Filtre su informe . . . 609
Exportar o imprimir informes . . . 610
Establezca el servidor SMTP para las notificaciones por correo electrónico . . . 610

Configure la opción para enviar informes por correo electrónico . . . 610
Gestione el repositorio del servidor SnapCenter . . . 611
Requisitos previos para proteger el repositorio de SnapCenter . . . 611
Realice un backup del repositorio de SnapCenter . . . 611
Ver los backups del repositorio de SnapCenter . . . 612
Restaurar el repositorio de la base de datos de SnapCenter . . . 612
Migre el repositorio de SnapCenter . . . 613
Restablecer la contraseña del repositorio de SnapCenter . . . 613
Gestione recursos de dominios que no son de confianza . . . 614
Modificar dominios que no son de confianza . . . 614
Cancele el registro de dominios de Active Directory que no son de confianza . . . 615
Gestione el sistema de almacenamiento . . . 615
Modifique la configuración del sistema de almacenamiento . . . 616
Elimine el sistema de almacenamiento . . . 618
Gestione la recogida de datos de EMS . . . 619
Detenga la recogida de datos de EMS . . . 619
Inicie la recogida de datos de EMS . . . 619
Cambie la programación de recogida de datos de EMS y SVM de destino . . . 619
Supervise el estado de recogida de datos de EMS . . . 620
Actualice el servidor de SnapCenter y los plugins . . . 621
Configure SnapCenter para la búsqueda de actualizaciones disponibles . . . 621
Actualizar el flujo de trabajo . . . 621
Rutas de actualización admitidas . . . 621
Actualice el servidor SnapCenter . . . 622
Actualice los paquetes de plugins . . . 624
Desinstale SnapCenter Server y los plugins . . . 626
Desinstale los paquetes de plugins de SnapCenter . . . 626
Requisitos previos para quitar un host . . . 626
Quitar un host . . . 627
Desinstale plugins mediante la interfaz gráfica de usuario de SnapCenter . . . 627
Desinstale los plugins de Windows mediante el cmdlet de PowerShell . . . 629
Desinstale los plugins localmente en un host . . . 629
Desinstale el paquete de plugins para Linux o AIX mediante la CLI . . . 630
Desinstale el servidor SnapCenter . . . 630
Automatización mediante API de REST . . . 631
Información general de las API de REST . . . 631
Cómo acceder a la API DE REST de SnapCenter de forma nativa . . . 631
Base de servicios web DE REST . . . 631
Recursos y representación estatal . . . 631
Extremos de URI . . . 632
Mensajes HTTP . . . 632
Formato JSON . . . 632
Variables de entrada que controlan una solicitud API . . . 632
Métodos HTTP . . . 632
Solicitar encabezados . . . 633

Solicitar el cuerpo 633
Filtrando objetos 633
Solicitando campos de objeto específicos 634
Ordenar objetos del conjunto de resultados 634
Paginación al recuperar objetos de una colección 634
Propiedades de tamaño 635
Interpretación de una respuesta API 636
Código de estado HTTP 636
Encabezados de respuesta 636
Cuerpo de respuesta 637
Errores 637
API de REST compatibles 638
Autor 638
Dominios 638
Trabajos 638
Configuración 639
Hosts 639
Recursos 639
Completos 639
Clones 639
Clanesplit 639
Grupos de recursos 640
Normativas 640
Reducida 640
Share 640
Complementos 640
Leídos 640
Alertas 640
RBAC 641
Configuración 641
CertificadosConfiguración 641
Repositorio 641
Cómo acceder a las API de REST a través de la página web de API de Swagger 641
Comience con la API DE REST 642
Hola Mundo 642
Avisos legales 644
Derechos de autor 644
Marcas comerciales 644
Estadounidenses 644
Política de privacidad 644
Traducción automática 644
Código abierto 644

# Documentación sobre el software SnapCenter

# Notas de la versión

Proporciona información importante sobre esta versión de SnapCenter Server y los paquetes de plugins de SnapCenter, incluidos los problemas solucionados, los problemas conocidos, las precauciones y las limitaciones.

Para obtener más información, consulte "Notas de la versión del software SnapCenter 4.5".

# Conceptos

## Información general de SnapCenter

El software SnapCenter es una plataforma sencilla, centralizada y escalable que proporciona protección de datos consistente con las aplicaciones para aplicaciones, bases de datos, sistemas de archivos host y máquinas virtuales que se ejecutan en sistemas ONTAP en cualquier parte del cloud híbrido.

SnapCenter aprovecha las tecnologías Snapshot, SnapRestore, FlexClone, SnapMirror y SnapVault de NetApp para proporcionar lo siguiente:

- Backup a disco rápido, con gestión eficiente del espacio y consistente con las aplicaciones
- Restauración rápida y granular, y recuperación consistente con las aplicaciones
- Clonado rápido y con un uso eficiente del espacio

SnapCenter incluye tanto SnapCenter Server como plugins individuales ligeros. Es posible automatizar la implementación de plugins en hosts de aplicaciones remotas, programar operaciones de backup, verificación y clonado, y supervisar todas las operaciones de protección de datos.

SnapCenter puede implementarse de las siguientes maneras:

- En las instalaciones para proteger lo siguiente:
  - Datos en sistemas principales ONTAP FAS o AFF replicados a sistemas secundarios ONTAP FAS o AFF
  - Datos en sistemas principales ONTAP Select
- En las instalaciones, en un cloud híbrido para proteger lo siguiente:
  - Datos en sistemas primarios ONTAP FAS o AFF y replicados a los sistemas secundarios Cloud Volumes ONTAP o NetApp Private Storage
- En un cloud público para proteger lo siguiente:
  - Datos sobre sistemas principales de Cloud Volumes ONTAP (antes ONTAP Cloud)

SnapCenter incluye las siguientes funciones clave:

- Protección de datos centralizada y coherente con las aplicaciones

  La protección de datos es compatible con Microsoft Exchange Server, Microsoft SQL Server, bases de datos de Oracle en Linux o AIX, base de datos SAP HANA y sistemas de archivos de host Windows que se ejecutan en sistemas ONTAP.

  La protección de datos también es compatible con otras aplicaciones y bases de datos estándar o personalizadas, ya que proporciona un marco de trabajo para crear plugins de SnapCenter definidos por el usuario. Esto permite proteger datos para otras aplicaciones y bases de datos desde el mismo panel único. Al aprovechar este marco, NetApp ha lanzado complementos personalizados de SnapCenter para IBM DB2, MongoDB, MySQL, etc. en el almacén de automatización de NetApp.

- Backups basados en normativas

  Los backups basados en políticas aprovechan la tecnología de copia de Snapshot de NetApp para crear

backups a disco rápidos, coherentes con las aplicaciones y con gestión eficiente del espacio. De manera opcional, puede automatizar la protección de estos backups en el almacenamiento secundario mediante las actualizaciones de las relaciones de protección existentes.

- Realice backups para varios recursos

  Puede realizar el backup de varios recursos (aplicaciones, bases de datos o sistemas de archivos de host) del mismo tipo, al mismo tiempo, mediante grupos de recursos de SnapCenter.

- Restauración y recuperación

  SnapCenter ofrece restauraciones rápidas y granulares de backups y recuperación basada en tiempo y coherente con las aplicaciones. Puede restaurar desde cualquier destino en el cloud híbrido.

- Clonado

  SnapCenter proporciona un clonado rápido y coherente con las aplicaciones que gestiona el espacio de manera eficiente, lo que permite un desarrollo de software acelerado. Puede clonar en cualquier destino en el cloud híbrido.

- Interfaz gráfica de usuario (GUI) de gestión de usuario única

  La interfaz gráfica de usuario de SnapCenter proporciona una interfaz única y única para gestionar backups y clones de un recurso en cualquier destino en el cloud híbrido.

- API DE REST, cmdlets de Windows, comandos de UNIX

  SnapCenter incluye API REST para la mayoría de las funcionalidades para la integración con cualquier software de orquestación, y para el uso de cmdlets de Windows PowerShell y la interfaz de línea de comandos.

- Consola de protección de datos y generación de informes centralizadas
- Control de acceso basado en roles (RBAC) para seguridad y delegación.
- Base de datos del repositorio con alta disponibilidad

  SnapCenter proporciona una base de datos de repositorio integrada con alta disponibilidad para almacenar todos los metadatos de backups.

- Instalación mediante inserción automatizada de plug-ins

  Puede automatizar una inserción remota de los plugins de SnapCenter desde el host del servidor de SnapCenter a los hosts de aplicaciones.

- Alta disponibilidad

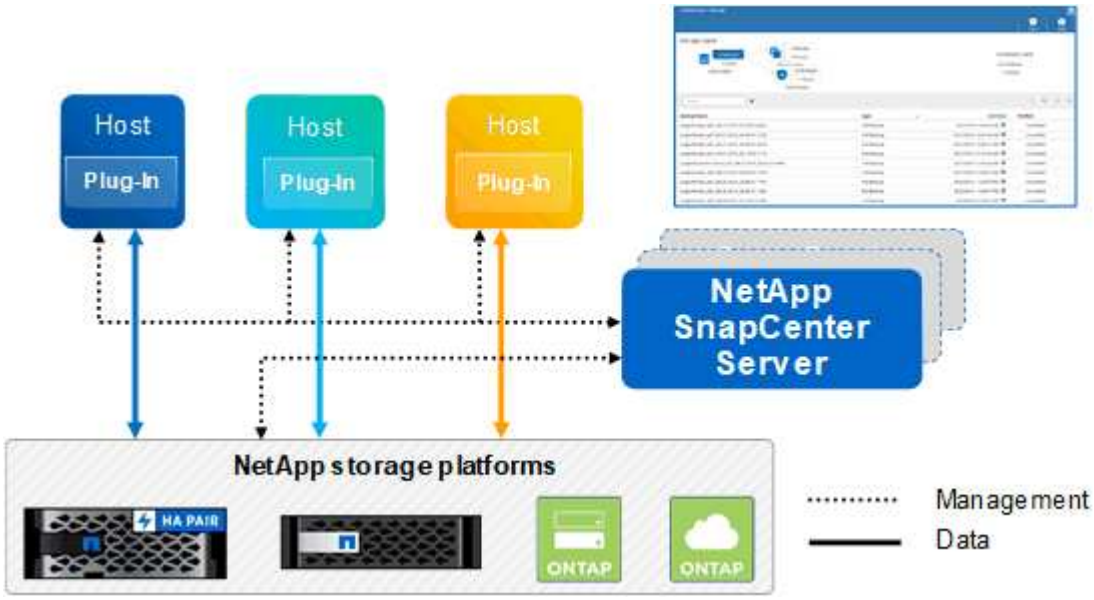
  La alta disponibilidad de SnapCenter se configura usando el equilibrador de carga externo (F5). Se admiten hasta dos nodos en el mismo centro de datos.

## Arquitectura SnapCenter

La plataforma de SnapCenter se basa en una arquitectura de varios niveles que incluye un servidor de gestión centralizado (servidor SnapCenter) y un host de complementos de SnapCenter.

SnapCenter admite centros de datos multisitio. El servidor de SnapCenter y el host del plugin pueden estar en

diferentes ubicaciones geográficas.




## Componentes de SnapCenter

SnapCenter consiste en los plugins de SnapCenter Server y SnapCenter. Debe instalar solo los plugins adecuados para los datos que desea proteger.

- Servidor SnapCenter
- Paquete de plugins de SnapCenter para Windows, que incluye los siguientes plugins:
  - Plugin de SnapCenter para Microsoft SQL Server
  - Plugin de SnapCenter para Microsoft Windows
  - Plugin de SnapCenter para Microsoft Exchange Server
  - Plugin de SnapCenter para base de datos SAP HANA
- Paquete de plugins de SnapCenter para Linux, que incluye los siguientes plugins:
  - Plugin de SnapCenter para base de datos de Oracle
  - Plugin de SnapCenter para base de datos SAP HANA
  - Complemento de SnapCenter para UNIX

> El plugin de SnapCenter para UNIX no es un plugin independiente y no se puede instalar de forma independiente. Este plugin se instala automáticamente cuando se instala el plugin de SnapCenter para base de datos de Oracle o el plugin de SnapCenter para base de datos SAP HANA.

- Paquete de plugins de SnapCenter para AIX, incluido los siguientes plugins:
  - Plugin de SnapCenter para base de datos de Oracle
  - Complemento de SnapCenter para UNIX

> El plugin de SnapCenter para UNIX no es un plugin independiente y no se puede instalar de forma independiente. Este plugin se instala automáticamente cuando se instala el plugin de SnapCenter para base de datos de Oracle.

- Plugins personalizados de SnapCenter

El plugin de SnapCenter para VMware vSphere, anteriormente conocido como Data Broker de NetApp, es un dispositivo virtual independiente que admite operaciones de protección de datos de SnapCenter en sistemas de archivos y bases de datos virtualizadas.

## Servidor SnapCenter

El servidor SnapCenter incluye un servidor web, una interfaz de usuario centralizada basada en HTML5, cmdlets de PowerShell, API DE REST y el repositorio de SnapCenter.

SnapCenter ofrece alta disponibilidad y escalado horizontal entre varias instancias de SnapCenter Server dentro de una sola interfaz de usuario. Puede lograr una alta disponibilidad mediante un equilibrador de carga externo (F5). Para entornos más grandes con miles de hosts, añadir varias instancias de SnapCenter Server puede ayudar a equilibrar la carga.

- Si utiliza el paquete de plugins de SnapCenter para Windows, el agente del host se ejecuta en SnapCenter Server y el host de plugins de Windows. El agente del host ejecuta las programaciones de forma nativa en el host Windows remoto; o bien, para instancias de Microsoft SQL Server, la programación se ejecuta en la instancia de SQL local.

  SnapCenter Server se comunica con los plugins de Windows a través del agente del host.

- Si utiliza el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX, las programaciones se ejecutan en SnapCenter Server como programaciones de tareas de Windows.
  - Para el plugin de SnapCenter para bases de datos de Oracle, el agente del host que se ejecuta en el host del servidor SnapCenter se comunica con el cargador de plugins (SPL) de SnapCenter que se ejecuta en el host Linux o AIX para realizar distintas operaciones de protección de datos.
  - Para el plugin de SnapCenter para bases de datos de SAP HANA y los plugins personalizados de SnapCenter, el servidor de SnapCenter se comunica con estos plugins a través del agente SCCore que se ejecuta en el host.

SnapCenter Server y los plugins se comunican con el agente del host mediante HTTPS.

La información sobre las operaciones de SnapCenter se almacena en el repositorio de SnapCenter.

## Plugins de SnapCenter

Cada plugin de SnapCenter admite entornos, bases de datos y aplicaciones específicas.

| Nombre de complemento | Incluido en el paquete de instalación | Requiere otros plugins | Instalado en el host | Plataforma compatible |
|---|---|---|---|---|
| Plugin para SQL Server | Paquete de plugins para Windows | Plugin para Windows | Host SQL Server | Windows |
| Plugin para Windows | Paquete de plugins para Windows | | Host Windows | Windows |
| Plugin para Exchange | Paquete de plugins para Windows | Plugin para Windows | Host Exchange Server | Windows |

| Nombre de complemento | Incluido en el paquete de instalación | Requiere otros plugins | Instalado en el host | Plataforma compatible |
|---|---|---|---|---|
| Plugin para base de datos de Oracle | Paquete de plugins para Linux y paquete de plugins para AIX | Complemento para UNIX | Host Oracle | Linux o AIX |
| Plugin para base de datos SAP HANA | Paquete de plugins para Linux y paquete de plugins para Windows | Plugin para UNIX o plugin para Windows | Host del cliente HDBSQL | Linux o Windows |
| Plugins personalizados | | Para backups del sistema de archivos, plugin para Windows | Host de aplicación personalizada | Linux o Windows |

El plugin de SnapCenter para VMware vSphere admite operaciones de backup y restauración consistentes con los fallos y consistentes con las máquinas virtuales (VM), almacenes de datos y discos de máquina virtual (VMDK), y admite los plugins específicos para aplicaciones de SnapCenter para proteger operaciones de backup y restauración consistentes con las aplicaciones para bases de datos y sistemas de archivos virtualizados.

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para los usuarios que utilizan SnapCenter 4.3 o posterior, el "Documentación del plugin de SnapCenter para VMware vSphere" Tiene información sobre la protección de bases de datos virtualizadas y sistemas de archivos mediante el plugin de SnapCenter basado en Linux para el dispositivo virtual VMware vSphere (formato de dispositivo virtual abierto).

### Funciones del plugin de SnapCenter para Microsoft SQL Server

- Automatiza las operaciones de backup, restauración y clonado para aplicaciones en bases de datos de Microsoft SQL Server en el entorno SnapCenter.
- Admite bases de datos de Microsoft SQL Server en VMDK y LUN de asignación de dispositivo sin formato (RDM) cuando se implementa el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter
- Admite el aprovisionamiento de solo recursos compartidos SMB. No se ofrece compatibilidad para realizar backups de bases de datos de SQL Server en recursos compartidos de SMB.
- Admite importar backups desde SnapManager para Microsoft SQL Server a SnapCenter.

### Funciones del plugin de SnapCenter para Microsoft Windows

- Posibilita la protección de datos para aplicaciones de otros plugins que se ejecutan en hosts Windows en el entorno de SnapCenter

- Automatiza las operaciones de backup, restauración y clonado para aplicaciones en sistemas de archivos de Microsoft en su entorno SnapCenter
- Admite el aprovisionamiento de almacenamiento, la consistencia de copias de Snapshot y la reclamación de espacio para hosts Windows

> El plugin para Windows aprovisiona recursos compartidos SMB y sistemas de archivos Windows en LUN de RDM físicos, pero no admite operaciones de backup para sistemas de archivos Windows en recursos compartidos SMB.

**Funciones del plugin de SnapCenter para Microsoft Exchange Server**

- Automatiza las operaciones de backup y restauración para aplicaciones en el entorno de SnapCenter para bases de datos y grupos de disponibilidad de bases de datos (DAG) de Microsoft Exchange Server
- Admite servidores Exchange virtualizados en LUN de RDM cuando se implementa el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter

**Funciones del plugin de SnapCenter para bases de datos de Oracle**

- Automatiza los backups, las restauraciones, la recuperación, la verificación, el montaje Operaciones de desmontaje y clonado de bases de datos de Oracle en el entorno de SnapCenter
- Sin embargo, no se proporciona integración con BR*Tools de SAP admite bases de datos Oracle para SAP

**Características del plugin de SnapCenter para UNIX**

- Permite al plugin para bases de datos de Oracle realizar operaciones de protección de datos en bases de datos de Oracle manejar la pila de almacenamiento del host subyacente en sistemas Linux o AIX
- Admite los protocolos de sistema de archivos de red (NFS) y red de área de almacenamiento (SAN) en un sistema de almacenamiento que ejecuta ONTAP.
- En el caso de los sistemas Linux, las bases de datos de Oracle en LUN de VMDK y RDM se admiten cuando se implementa el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter.
- Admite Mount Guard para AIX en sistemas DE archivos SAN y diseño de LVM.
- Admite el sistema de archivos mejorado Journaled (JFS2) con registro en línea en sistemas DE archivos SAN y diseño LVM sólo para sistemas AIX.

  Se admiten los dispositivos nativos DE SAN, sistemas de archivos y diseños de LVM creados en dispositivos SAN.

**Funciones del plugin de SnapCenter para base de datos SAP HANA**

- Automatiza el backup, la restauración y la clonado de bases de datos de SAP HANA en su entorno SnapCenter

**Funciones de los plugins personalizados de SnapCenter**

- Admite plugins personalizados para gestionar aplicaciones o bases de datos que otros plugins de SnapCenter no admiten. No se incluyen los plugins personalizados como parte de la instalación de SnapCenter.

- Admite la creación de copias reflejadas de conjuntos de backup en otro volumen y la ejecución de la replicación de backup de disco a disco.
- Es compatible con entornos Windows y Linux. En los entornos de Windows, las aplicaciones personalizadas a través de plugins personalizados pueden utilizar, opcionalmente, el plugin de SnapCenter para Microsoft Windows con el fin de realizar backups consistentes del sistema de archivos.

Los plugins personalizados de MySQL, DB2 y MongoDB reciben soporte exclusivamente a través de las comunidades de NetApp.

NetApp admite la funcionalidad de crear y utilizar plugins personalizados; sin embargo, los plugins personalizados que usted crea no son compatibles con NetApp.

Para obtener más información, consulte "Desarrolle un complemento para la aplicación"

### Repositorio de SnapCenter

El repositorio de SnapCenter, que a veces se denomina base de datos NSM, almacena información y metadatos para cada operación SnapCenter.

La base de datos del repositorio de MySQL Server se instala de manera predeterminada cuando se instala el servidor SnapCenter. Si MySQL Server ya está instalado y está realizando una instalación nueva de SnapCenter Server, deberá desinstalar MySQL Server.

SnapCenter admite MySQL Server 5.7.25 o posterior como base de datos del repositorio de SnapCenter. Si utilizaba una versión anterior de MySQL Server con una versión anterior de SnapCenter, durante la actualización de SnapCenter, se actualizó el servidor MySQL a la versión 5.7.25 o posterior.

El repositorio de SnapCenter almacena la siguiente información y metadatos:

- Metadatos de backup, clonado, restauración y verificación
- Información sobre informes, trabajos y eventos
- Información sobre el host y los plugins
- Detalles de roles, usuarios y permisos
- Información de conexiones del sistema de almacenamiento

# Funciones de seguridad

## SnapCenter emplea funciones de seguridad y autenticación estrictas para permitirle mantener seguros los datos.

SnapCenter incluye las siguientes funciones de seguridad:

- Toda la comunicación con SnapCenter utiliza HTTP sobre SSL (HTTPS).
- Todas las credenciales en SnapCenter están protegidas con el cifrado Advanced Encryption Standard (AES).
- SnapCenter utiliza algoritmos de seguridad que cumplen con el estándar de procesamiento de información federal (FIPS).
- SnapCenter admite el uso de certificados de CA autorizados que proporciona el cliente.
- SnapCenter 4.1.1 o posterior admite la comunicación de seguridad de la capa de transporte (TLS) 1.2 con

ONTAP. También puede usar comunicación TLS 1.2 entre clientes y servidores.

- SnapCenter se instala dentro del firewall de su compañía para habilitar el acceso al servidor SnapCenter y permitir la comunicación entre SnapCenter Server y los plugins.
- El acceso a la API de SnapCenter y las operaciones utiliza tokens cifrados con el cifrado AES, que caducan luego de 24 horas.
- SnapCenter se integra con Windows Active Directory para el inicio de sesión y RBAC que rige los permisos de acceso.
- Los cmdlets de PowerShell de SnapCenter están protegidos por la sesión.
- Después de un período predeterminado de 15 minutos de inactividad, SnapCenter advierte que la sesión se cerrará en 5 minutos. Después de 20 minutos de inactividad, SnapCenter cierra la sesión, que debe volver a iniciarse. Es posible modificar el período de cierre de sesión por inactividad.
- El inicio de sesión se deshabilita temporalmente luego de 5 o más intentos incorrectos de inicio de sesión.

### Descripción general del certificado CA

El instalador de SnapCenter Server activa la compatibilidad centralizada con certificados SSL durante la instalación. Para mejorar la comunicación segura entre el servidor y el plugin, SnapCenter admite el uso de certificados de CA autorizados proporcionados por el cliente.

Debe implementar certificados de CA después de instalar SnapCenter Server y los respectivos plugins. Para obtener más información, consulte "Genere un archivo CSR de certificado de CA".

También puede implementar un certificado CA para el complemento SnapCenter para VMware vSphere. Para obtener más información, consulte "Crear e importar certificados" .

# Control de acceso basado en roles (RBAC) de SnapCenter

## Tipos de RBAC

El control de acceso basado en roles (RBAC) de SnapCenter y los permisos de ONTAP permiten que los administradores de SnapCenter delegen el control de los recursos de SnapCenter a diferentes usuarios o grupos de usuarios. Este acceso con gestión central otorga a los administradores de aplicaciones la posibilidad de trabajar con seguridad dentro de entornos delegados.

Es posible crear y modificar roles, y añadir acceso a recursos para usuarios en cualquier momento, pero cuando configura SnapCenter por primera vez, debe añadir al menos usuarios o grupos de Active Directory a roles, y luego añadir acceso a recursos para esos usuarios o grupos.

No se puede usar SnapCenter para cuentas de usuarios o grupos. Creó cuentas de usuario o de grupo en Active Directory mediante el sistema operativo o la base de datos.

SnapCenter usa los siguientes tipos de control de acceso basado en roles:

- RBAC de SnapCenter
- RBAC para plugin de SnapCenter (para algunos plugins)
- RBAC en el nivel de aplicaciones
- Permisos de ONTAP

## RBAC de SnapCenter

#### Roles y permisos

SnapCenter incluye roles predefinidos con permisos ya asignados. Es posible asignar usuarios o grupos de usuarios a estos roles. También es posible crear nuevos roles y gestionar los permisos y los usuarios.

### Asignación de permisos a usuarios o grupos

Es posible asignar permisos a usuarios o grupos para que tengan acceso a objetos de SnapCenter, como hosts, conexiones de almacenamiento y grupos de recursos. No es posible cambiar los permisos del rol SnapCenterAdmin.

Se pueden asignar permisos de RBAC a usuarios y grupos dentro del mismo bosque y a usuarios de distintos bosques. No es posible asignar permisos de RBAC a usuarios que pertenecen a grupos anidados en diferentes bosques.

Si se crea un rol personalizado, este debe contener todos los permisos del rol SnapCenter Admin. Si solo se copian algunos de los permisos, como Host add o Host remove, no se pueden ejecutar tales operaciones.

#### Autenticación

Los usuarios deben proporcionar autenticación durante el inicio de sesión, ya sea desde la interfaz gráfica de usuario o mediante cmdlets de PowerShell. Si un usuario es parte de más de un rol, después de introducir las credenciales de inicio de sesión, se le solicita que especifique el rol que desea usar. Los usuarios también deben proporcionar autenticación para ejecutar las API.

### RBAC en el nivel de aplicaciones

SnapCenter usa credenciales para verificar que los usuarios de SnapCenter autorizados también tengan permisos en el nivel de aplicaciones.

Por ejemplo, para ejecutar operaciones de copia de Snapshot y protección de datos en un entorno de SQL Server, se deben configurar las credenciales con las credenciales de Windows o SQL correspondientes. El servidor de SnapCenter autentica el conjunto de credenciales con cualquiera de estos métodos. Para ejecutar operaciones de copia de Snapshot y protección de datos en un entorno de sistema de archivos de Windows sobre almacenamiento ONTAP, el rol SnapCenter Admin debe tener privilegios de administrador en el host de Windows.

Del mismo modo, si se desean ejecutar operaciones de protección de datos en una base de datos de Oracle y la autenticación del sistema operativo está deshabilitada en el host de base de datos, se deben configurar las credenciales con la base de datos de Oracle o las credenciales de ASM de Oracle. El servidor de SnapCenter autentica el conjunto de credenciales mediante uno de estos métodos, según la operación.

### Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere

Cuando se utiliza el plugin de SnapCenter VMware para protección de datos coherente con máquinas virtuales, vCenter Server ofrece un nivel adicional de control de acceso basado en roles. El plugin de SnapCenter de VMware es compatible con el control de acceso basado en roles de vCenter Server y de Data ONTAP.

Para obtener más información, consulte "Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere"

### Permisos de ONTAP

Es necesario crear una cuenta de vsadmin con los permisos requeridos para acceder al sistema de almacenamiento.

Para obtener más información sobre cómo crear la cuenta y asignar permisos, consulte "Cree un rol de clúster de ONTAP con privilegios mínimos"

## Permisos y roles de RBAC

El control de acceso basado en roles de SnapCenter permite crear roles y asignar permisos a esos roles para luego asignar usuarios o grupos de usuarios a ellos. Esto permite que los administradores de SnapCenter creen un entorno gestionado de manera centralizada, mientras que los administradores de aplicaciones pueden gestionar trabajos de protección de datos. SnapCenter se envía con algunos roles y permisos predefinidos.

### Roles de SnapCenter

SnapCenter se envía con los siguientes roles predefinidos. Es posible asignar usuarios y grupos a estos roles, o bien crear roles nuevos.

Cuando se asigna un rol a un usuario, solo los trabajos relevantes para ese usuario son visibles en la página Jobs, a menos que se haya asignado el rol SnapCenter Admin.

- App Backup y Clone Admin
- Backup y Clone Viewer
- Administrador de infraestructuras
- Administrador de SnapCenter

### Roles del plugin de SnapCenter para VMware vSphere

Para gestionar la protección de datos coherente con las máquinas virtuales de máquinas virtuales, VMDK y almacenes de datos, el plugin de SnapCenter para VMware vSphere crea los siguientes roles en vCenter:

- Administrador de SCV
- Vista de VCS
- Backup de SCV
- Restauración de SCV
- Restauración de archivos invitados de SCV

Para obtener más información, consulte "Tipos de RBAC para usuarios del plugin de SnapCenter para VMware vSphere"

**Mejor práctica:** NetApp recomienda crear un rol de ONTAP para las operaciones del plugin de SnapCenter para VMware vSphere y asignarle todos los privilegios necesarios.

**Permisos de SnapCenter**

SnapCenter otorga los siguientes permisos:

- Grupo de recursos
- Política
- Backup
- Host
- Conexión de almacenamiento
- Clonar
- Aprovisionamiento (solo para bases de datos Microsoft SQL)
- Consola
- Leídos
- Restaurar
  - Restauración de volúmenes completa (solo para plugins personalizados)
- Recurso

  El administrador debe otorgar privilegios de plugins para que los no administradores realicen operaciones de detección de recursos.

- Instalar o desinstalar plugins

  Cuando habilita los permisos de instalación de plugins, también debe modificar el permiso del host para permitir lecturas y actualizaciones.

- Migración
- Montaje (solo para bases de datos de Oracle)
- Desmontaje (solo para bases de datos de Oracle)
- Monitor de trabajos

  El permiso Monitor de trabajo permite a los miembros de diferentes roles ver las operaciones en todos los objetos a los que están asignados.

## Roles y permisos predefinidos de SnapCenter

SnapCenter incluye de forma predeterminada varios roles predefinidos, cada uno con un conjunto de permisos ya habilitados. Al configurar y administrar el control de acceso basado en roles, se pueden usar estos roles predefinidos o crear roles nuevos.

SnapCenter incluye los siguientes roles predefinidos:

- SnapCenter Admin
- App Backup and Clone Admin
- Backup and Clone Viewer
- Infrastructure Admin

Cuando se agrega un usuario a un rol, se le debe asignar el permiso StorageConnection para permitir la comunicación con Storage Virtual Machine (SVM) o asignarle una SVM al usuario para habilitar su uso. El permiso Storage Connection permite que los usuarios creen conexiones de SVM.

Por ejemplo, un usuario con el rol SnapCenter Admin puede crear conexiones de SVM y asignarlas a un usuario con el rol App Backup and Clone Admin, cuyos permisos predeterminados no incluyen la creación o edición de SVM. Si no hay una conexión de SVM, los usuarios no pueden ejecutar ninguna operación de backup, clonado o restauración.

**SnapCenter Admin**

El rol SnapCenter Admin tiene todos los permisos habilitados. No es posible modificar los permisos de este rol. Se pueden agregar usuarios y grupos al rol o quitarlos.

**App Backup and Clone Admin**

El rol App Backup and Clone Admin tiene los permisos necesarios para ejecutar acciones administrativas para tareas vinculadas con el backup y la clonado de aplicaciones. Este rol no tiene permisos para gestión de hosts, aprovisionamiento, gestión de conexiones de almacenamiento o instalación remota.

| Permisos | Activado | Cree | Lea | Actualizar | Eliminar |
|---|---|---|---|---|---|
| Grupo de recursos | No aplicable | Sí | Sí | Sí | Sí |
| Política | No aplicable | Sí | Sí | Sí | Sí |
| Backup | No aplicable | Sí | Sí | Sí | Sí |
| Host | No aplicable | Sí | Sí | Sí | Sí |
| Conexión de almacenamiento | No aplicable | No | Sí | No | No |
| Clonar | No aplicable | Sí | Sí | Sí | Sí |
| Provisionamiento | No aplicable | No | Sí | No | No |
| Consola | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Leídos | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Restaurar | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Recurso | Sí | Sí | Sí | Sí | Sí |
| Instalar/desinstalar plugins | No | No aplicable | | No aplicable | No aplicable |

| Permisos | Activado | Cree | Lea | Actualizar | Eliminar |
|---|---|---|---|---|---|
| Migración | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Montaje | Sí | Sí | No aplicable | No aplicable | No aplicable |
| Desmontar | Sí | Sí | No aplicable | No aplicable | No aplicable |
| Restaurar volumen completo | No | No | No aplicable | No aplicable | No aplicable |
| Monitor de trabajos | Sí | No aplicable | No aplicable | No aplicable | No aplicable |

**Backup and Clone Viewer**

El rol Backup and Clone Viewer tiene una vista de solo lectura de todos los permisos. Este rol también tiene permisos habilitados para detección, generación de informes y acceso a la consola.

| Permisos | Activado | Cree | Lea | Actualizar | Eliminar |
|---|---|---|---|---|---|
| Grupo de recursos | No aplicable | No | Sí | No | No |
| Política | No aplicable | No | Sí | No | No |
| Backup | No aplicable | No | Sí | No | No |
| Host | No aplicable | No | Sí | No | No |
| Conexión de almacenamiento | No aplicable | No | Sí | No | No |
| Clonar | No aplicable | No | Sí | No | No |
| Provisionamiento | No aplicable | No | Sí | No | No |
| Consola | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Leídos | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Restaurar | No | No | No aplicable | No aplicable | No aplicable |
| Recurso | No | No | Sí | Sí | No |

| Permisos | Activado | Cree | Lea | Actualizar | Eliminar |
|---|---|---|---|---|---|
| Instalar/desinstalar plugins | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Migración | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Montaje | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Desmontar | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Restaurar volumen completo | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Monitor de trabajos | Sí | No aplicable | No aplicable | No aplicable | No aplicable |

**Infrastructure Admin**

El rol Infrastructure Admin tiene permisos habilitados para gestión de hosts, administración del almacenamiento, aprovisionamiento, grupos de recursos, informes de instalación remota, Y acceso a la consola.

| Permisos | Activado | Cree | Lea | Actualizar | Eliminar |
|---|---|---|---|---|---|
| Grupo de recursos | No aplicable | Sí | Sí | Sí | Sí |
| Política | No aplicable | No | Sí | Sí | Sí |
| Backup | No aplicable | Sí | Sí | Sí | Sí |
| Host | No aplicable | Sí | Sí | Sí | Sí |
| Conexión de almacenamiento | No aplicable | Sí | Sí | Sí | Sí |
| Clonar | No aplicable | No | Sí | No | No |
| Provisionamiento | No aplicable | Sí | Sí | Sí | Sí |
| Consola | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Leídos | Sí | No aplicable | No aplicable | No aplicable | No aplicable |

| Permisos | Activado | Cree | Lea | Actualizar | Eliminar |
|---|---|---|---|---|---|
| Restaurar | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Recurso | Sí | Sí | Sí | Sí | Sí |
| Instalar/desinstalar plugins | Sí | No aplicable | No aplicable | No aplicable | No aplicable |
| Migración | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Montaje | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Desmontar | No | No aplicable | No aplicable | No aplicable | No aplicable |
| Restaurar volumen completo | No | No | No aplicable | No aplicable | No aplicable |
| Monitor de trabajos | Sí | No aplicable | No aplicable | No aplicable | No aplicable |

# Recursos, grupos de recursos y políticas

Antes de usar SnapCenter, es necesariol comprender ciertos conceptos básicos vinculados con las operaciones de backup, clonado y restauración que se ejecutan. El usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- **Los recursos** suelen ser las bases de datos, los sistemas de archivos Windows o los recursos compartidos de archivos de los que se realiza una copia de seguridad o se clonan con SnapCenter.

  No obstante, según cuál sea el entorno, los recursos también pueden ser instancias de bases de datos, grupos de disponibilidad de Microsoft SQL Server, bases de datos de Oracle, base de datos de Oracle RAC, sistemas de archivos Windows o un grupo de aplicaciones personalizadas.

- Un **grupo de recursos** es una colección de recursos en un host o clúster. El grupo de recursos también puede contener recursos de varios hosts y varios clústeres.

  Cuando se ejecuta una operación con un grupo de recursos, esta se aplica a todos los recursos definidos en el grupo de acuerdo con la programación especificada para el grupo de recursos.

  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También se pueden configurar backups programados para recursos individuales o grupos de recursos.

  Si se coloca un host de un grupo de recursos compartidos en modo de mantenimiento y existen programaciones asociadas con el mismo grupo, se suspenden todas las operaciones programadas en todos los demás hosts del grupo de recursos compartidos.

Es conveniente usar un plugin de base de datos para el backup de bases de datos, un plugin de sistema de archivos para el backup de sistemas de archivos y el plugin de SnapCenter para VMware vSphere para el backup de máquinas virtuales y almacenes de datos.

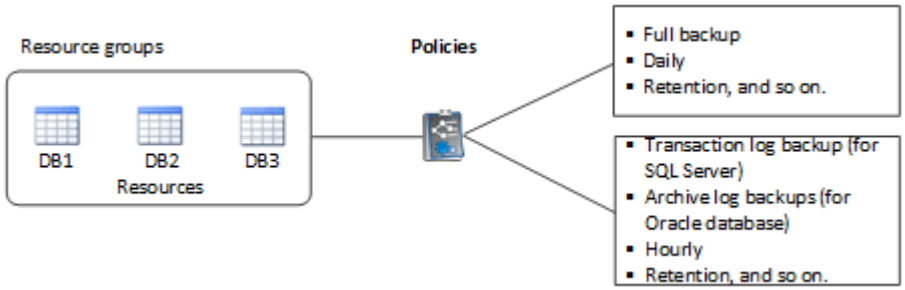
- **Las directivas** especifican la frecuencia de copia de seguridad, la retención de copias, la replicación, las secuencias de comandos y otras características de las operaciones de protección de datos.

  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. También es posible seleccionar una política al ejecutar un backup bajo demanda.

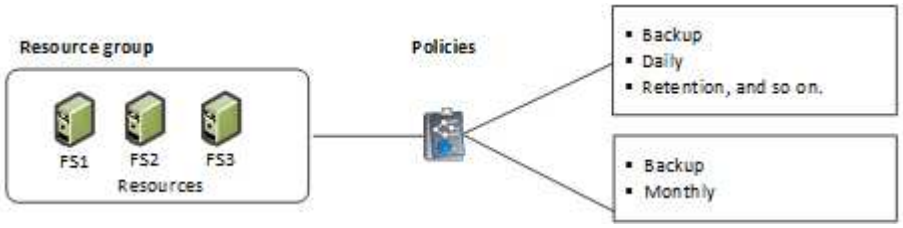
Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos o todos los sistemas de archivos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria.

Cuando se crea el grupo de recursos y se vinculan las políticas, es posible configurar el grupo de recursos para que se ejecute un backup completo todos los días, y agregar una programación que ejecute un backup del registro por hora.

En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:




En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para los sistemas de archivos Windows:




# Scripts previos y posteriores

Es posible usar scripts previos y posteriores como parte de las operaciones de protección de datos. Estos scripts permiten la automatización antes o después del trabajo de protección de datos. Por ejemplo, se puede incluir un script para notificar automáticamente si hay fallos o advertencias en un trabajo de protección de datos. Para configurar scripts previos y posteriores, es necesario comprender algunos de los requisitos para crearlos.

## Tipos de scripts compatibles

Se admiten los siguientes tipos de scripts para Windows:

- Archivos de lotes
- Scripts de PowerShell
- Scripts Perl

Los siguientes tipos de scripts se admiten para UNIX:

- Scripts Perl
- Scripts Python
- Scripts de shell

Junto con el shell bash predeterminado, también se admiten otros shell como sh-shell, k-shell y c-shell.

## Ruta del script

Todos los scripts previos y posteriores que se ejecutan como parte de las operaciones de SnapCenter, en sistemas de almacenamiento virtualizados y no virtualizados, se ejecutan en el host del plugin.

- Los scripts de Windows deben encontrarse en el host del plugin o en un recurso compartido de SMB al que pueda acceder el host del plugin.
- Los scripts de UNIX deben encontrarse en el host del plugin.

La ruta de acceso del script se valida en el momento en que se ejecuta el script.

## Dónde especificar scripts

Los scripts se especifican en las políticas de backup. Cuando se inicia una tarea de backup, la política asocia automáticamente el script con los recursos que se incluirán en el backup. Al crear una política de backup, se pueden especificar los argumentos de script previo y script posterior.

Sólo para Windows, puede especificar varios scripts. Debe pulsar **Enter** después de cada ruta de script para enumerar cada script en una línea diferente. No se admite el uso de punto y coma (;). Es posible especificar varios scripts previos y posteriores. Un script individual se puede codificar como script previo y script posterior, y puede llamar a otros scripts.

Para UNIX, no puede especificar varios scripts.

## Tiempo de espera de scripts

Para Windows, el tiempo de espera está configurado en 15 minutos y no puede modificarse.

Para UNIX, el tiempo de espera se establece de forma predeterminada en 60 segundos. Puede modificar el valor del tiempo de espera.

### Salida de script

El directorio predeterminado para los archivos de salida scripts previos y posteriores de Windows es Windows\System32.

No hay una ubicación predeterminada para los scripts previos y posteriores de UNIX. Puede redirigir el archivo de salida a cualquier ubicación preferida.

# Automatización de SnapCenter mediante API de REST

Es posible utilizar API DE REST para realizar varias operaciones de gestión de SnapCenter. Las API DE REST se exponen a través de la página web de Swagger. Es posible acceder a la página web de Swagger para ver la documentación de la API DE REST, y también para emitir manualmente una llamada API. Es posible usar la API DE REST para ayudar a gestionar SnapCenter Server o el host de SnapCenter vSphere.

| Las API DE REST para… | Se encuentran en… |
|---|---|
| Servidor SnapCenter | \Https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/ |
| Plugin de SnapCenter para VMware vSphere | \Https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/api/swagger-ui.html# |

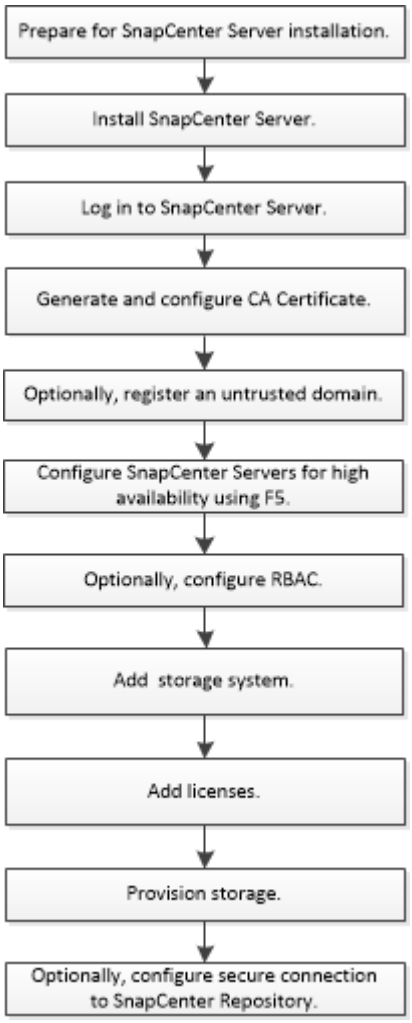
Para obtener más información sobre las API de REST de SnapCenter, consulte "Información general de las API de REST"

Para obtener información sobre las API de REST del plugin de SnapCenter para VMware vSphere, consulte "API de REST del plugin de SnapCenter para VMware vSphere"

# Instalación del servidor SnapCenter

## Flujo de trabajo de instalación

El flujo de trabajo muestra las distintas tareas necesarias para instalar y configurar el servidor SnapCenter.




## Prepare la instalación del servidor SnapCenter

### Requisitos de dominio y grupo de trabajo

El servidor SnapCenter se puede instalar en sistemas que estén en un dominio o en un grupo de trabajo. El usuario utilizado para la instalación debe tener privilegios de administrador en el equipo en caso de grupo de trabajo y dominio.

Para instalar los plugins de SnapCenter Server y SnapCenter en hosts de Windows, debe usar uno de los siguientes elementos:

- **Dominio de Active Directory**

  Debe usar un usuario de dominio con derechos de administrador local. El usuario de dominio debe ser

miembro del grupo de administrador local en el host de Windows.

- **Grupos de trabajo**

  Debe utilizar una cuenta local que tenga derechos de administrador local.

Mientras que las confianzas de dominio, bosques de multidominio y confianzas entre dominios son compatibles, los dominios entre bosques no lo son. La documentación de Microsoft acerca de Dominios y confianzas de Active Directory contiene más información.

Tras instalar el servidor SnapCenter, no debe cambiar el dominio en el que se encuentra el host SnapCenter. Si quita el host de SnapCenter Server del dominio en el que estaba cuando se instaló el servidor SnapCenter y, a continuación, intenta desinstalar SnapCenter Server, la operación de desinstalación fracasará.

## Requisitos de espacio y de tamaño

Antes de instalar el servidor SnapCenter, debería estar familiarizado con los requisitos de espacio y tamaño. También debe aplicar las actualizaciones de sistema y seguridad disponibles.

| Elemento | Requisitos |
| --- | --- |
| Sistemas operativos | Microsoft Windows<br><br>Solo se admiten las versiones en inglés, alemán, japonés y chino simplificado de los sistemas operativos.<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |
| Recuento de CPU mínimo | 4 núcleos |
| RAM mínimo | 8 GB<br><br>El grupo de buffers de MySQL Server utiliza el 20 por ciento de la RAM total. |
| Espacio mínimo en disco duro para el software y los registros del servidor SnapCenter | 4 GB<br><br>Si tiene el repositorio de SnapCenter en la misma unidad donde está instalado el servidor SnapCenter, se recomienda tener 10 GB. |

| Elemento | Requisitos |
| --- | --- |
| Espacio en disco duro mínimo para el repositorio de SnapCenter | 6 GB<br><br>NOTA: Si tiene el servidor SnapCenter en la misma unidad en la que está instalado el repositorio de SnapCenter, se recomienda tener 10 GB. |
| Paquetes de software obligatorios | • Microsoft .NET Framework 4.5.2 o posterior<br>• Windows Management Framework (WMF) 4.0 o posterior<br>• PowerShell 4.0 o posterior<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |

## Requisitos del host SAN

Si el host de SnapCenter forma parte de un entorno FC/iSCSI, puede que tenga que instalar software adicionales en el sistema para habilitar el acceso al almacenamiento ONTAP.

SnapCenter no incluye las utilidades de host ni DSM. Si el host de SnapCenter forma parte de un entorno SAN, puede tener que instalar y configurar el siguiente software:

- Utilidades de host

  Las utilidades de host son compatibles con FC e iSCSI, y le permiten usar MPIO en sus servidores Windows. Para obtener más información, consulte "Documentación de utilidades de host".

- Microsoft DSM para Windows MPIO

  Este software funciona con controladores Windows MPIO para gestionar varias rutas entre equipos host de Windows y NetApp.

  Se requiere un DSM para configuraciones de alta disponibilidad.

  Si estaba utilizando ONTAP DSM, debe migrar a Microsoft DSM. Para obtener más información, consulte "Cómo migrar desde ONTAP DSM a Microsoft DSM".

## Sistemas de almacenamiento y aplicaciones compatibles

Debe conocer cuáles son los sistemas de almacenamiento, las aplicaciones y las bases de datos compatibles.

- SnapCenter admite ONTAP 8.3.0 y versiones posteriores para proteger sus datos.
- SnapCenter es compatible con Amazon FSX para NetApp ONTAP de la versión de revisión P1 del

software SnapCenter 4.5.

Si se utiliza Amazon FSX para ONTAP de NetApp, asegúrese de que los plugins del host del servidor SnapCenter se actualicen a la versión de revisión 4.5 P1 para realizar operaciones de protección de datos.

Para obtener más información sobre Amazon FSX para ONTAP de NetApp, consulte "Documentación de Amazon FSX para ONTAP de NetApp".

- SnapCenter admite la protección de distintas aplicaciones y bases de datos.

  Para obtener información detallada sobre las aplicaciones y bases de datos compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

## Exploradores compatibles

El software SnapCenter se puede usar en diversos exploradores.

- Cromo

  Si utiliza v66, es posible que no se pueda iniciar la interfaz gráfica de usuario de SnapCenter.

- Internet Explorer

  La interfaz de usuario de SnapCenter no se carga correctamente si se utiliza IE 10 o versiones anteriores. Debe actualizar a IE 11.

  - Tan solo se ofrece compatibilidad para las funciones de seguridad de nivel predeterminado.

    Realizar cambios en la configuración de seguridad de Internet Explorer puede dar como resultado problemas significativos de visualización para el explorador.

  - Es necesario deshabilitar la vista de compatibilidad de Internet Explorer.

- Microsoft Edge

Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

## Requisitos de conexión y puerto

Debe asegurarse de que se cumplan los requisitos de conexiones y puertos antes de instalar SnapCenter Server y los plugins de aplicación o base de datos.

- Las aplicaciones no pueden compartir los puertos.

  Cada puerto debe ser dedicado a la aplicación adecuada.

- En el caso de los puertos personalizables, puede seleccionar un puerto personalizado durante la instalación si no quiere usar el predeterminado.

  Puede cambiar un puerto de plugin después de la instalación usando el asistente Modify host.

- En el caso de los puertos fijos, tiene que aceptar el número de puerto predeterminado.
- Servidores de seguridad

- Firewalls, proxies u otros dispositivos de red no deben interferir con las conexiones.
- Si especifica un puerto personalizado al instalar SnapCenter, tendrá que añadir un regla de firewall en el host del plugin para dicho puerto en el cargador del plugin de SnapCenter.

En la tabla siguiente se enumeran los distintos puertos y sus valores predeterminados.

| Tipo de puerto | Puerto predeterminado |
|---|---|
| Puerto SnapCenter | 8146 (HTTPS), bidireccional, personalizable, como en la URL *https://server:8146*<br><br>Se usa para la comunicación entre el cliente SnapCenter (el usuario de SnapCenter) y el servidor SnapCenter. También se utiliza para establecer la comunicación de los hosts del plugin con SnapCenter Server.<br><br>Para personalizar el puerto, consulte "Instale el servidor SnapCenter con el asistente de instalación." |
| Puerto de comunicación SMCore de SnapCenter | 8145 (HTTPS), bidireccional, personalizable<br><br>El puerto se utiliza para establecer la comunicación entre SnapCenter Server y los hosts en los que se han instalado los plugins de SnapCenter.<br><br>Para personalizar el puerto, consulte "Instale el servidor SnapCenter con el asistente de instalación." |
| Puerto MySQL | 3306 (HTTPS), bidireccional<br><br>El puerto se utiliza para establecer la comunicación entre SnapCenter y la base de datos del repositorio MySQL.<br><br>Puede crear conexiones seguras desde el servidor SnapCenter al servidor MySQL. "Leer más" |

| Tipo de puerto | Puerto predeterminado |
| --- | --- |
| Hosts de plugins de Windows | 135 DE FEBRERO DE 445 (TCP)<br><br>Además de los puertos 135 y 445, el intervalo de puertos dinámico especificado por Microsoft también debería estar abierto. Operaciones de instalación remota Utilice el servicio Instrumental de administración de Windows (WMI), que busca dinámicamente este intervalo de puertos.<br><br>Para obtener información sobre el intervalo de puertos dinámicos admitido, consulte "Descripción general del servicio y requisitos de puertos de red para Windows"<br><br>Los puertos se utilizan para establecer la comunicación entre SnapCenter Server y el host en el que se está instalando el plugin. Para insertar los archivos binarios de paquetes de plugins en los hosts de plugin de Windows, los puertos deben abrirse con cuidado en el host del plugin y se pueden cerrar después de su instalación. |
| Hosts de plugins de Linux o AIX | 22 (SSH)<br><br>Los puertos se utilizan para establecer la comunicación entre SnapCenter Server y el host en el que se está instalando el plugin. Los puertos los utiliza SnapCenter para copiar archivos binarios de paquetes de plugin en los hosts de plugin de Linux o AIX y se deben abrir o ejecutar desde el firewall o las iptables. |
| Paquete de plugins de SnapCenter para Windows, paquete de plugins de SnapCenter para Linux o paquete de plugins de SnapCenter para AIX | 8145 (HTTPS), bidireccional, personalizable<br><br>El puerto se utiliza para establecer la comunicación entre SMCore y los hosts en los que se ha instalado el paquete de plugins.<br><br>La ruta de comunicación también debe estar abierta entre el LIF de gestión de SVM y el servidor SnapCenter.<br><br>Para personalizar el puerto, consulte "Añada hosts e instale el plugin de SnapCenter para Microsoft Windows" o. "Añada hosts e instale el paquete de plugins de SnapCenter para Linux o AIX." |

| Tipo de puerto | Puerto predeterminado |
| --- | --- |
| Plugin de SnapCenter para base de datos de Oracle | 27216, personalizable<br><br>El puerto de JDBC predeterminado, lo utiliza el plugin para Oracle para conectarse a la base de datos de Oracle.<br><br>Para personalizar el puerto, consulte "Añada hosts e instale el paquete de plugins de SnapCenter para Linux o AIX." |
| Plugins personalizados para SnapCenter | 9090 (HTTPS), fija<br><br>Se trata de un puerto interno que se usa solo en el host del plugin personalizado; no son obligatorias las excepciones de firewall.<br><br>La comunicación entre SnapCenter Server y los plugins personalizados pasa a través del puerto 8145. |
| Puerto de comunicación del clúster de ONTAP o de SVM | 443 (HTTPS), bidirectional80 (HTTP), bidireccional<br><br>El puerto se utiliza en SAL (capa de abstracción del almacenamiento) para establecer la comunicación entre el host que ejecuta SnapCenter Server y SVM. Actualmente, el puerto también se utiliza en SAL en SnapCenter para los hosts del plugin de Windows para establecer la comunicación entre el host del plugin de SnapCenter y SVM. |
| Plugin de SnapCenter para base de datos SAP HANA vCode Spell Checkports | 3instance_number13 o 3instance_number15, HTTP o HTTPS, bidireccional y personalizable<br><br>Para un tenant único de un contenedor de base de datos multitenant (MDC), el número del puerto termina en 13; para los que no son MDC, el número de puerto termina en 15.<br><br>Por ejemplo, 32013 es el número de puerto para la instancia 20 y 31015 es el número de puerto para la instancia 10.<br><br>Para personalizar el puerto, consulte "Añada hosts e instale paquetes de plugins en hosts remotos." |

| Tipo de puerto | Puerto predeterminado |
| --- | --- |
| Puerto de comunicación del controlador de dominio | Consulte la documentación de Microsoft para identificar los puertos que se deben abrir en el firewall de un controlador de dominio para que la autenticación funcione correctamente.<br><br>Es necesario abrir los puertos requeridos por Microsoft en el controlador de dominio para que SnapCenter Server, los hosts del plugin u otro cliente de Windows puedan autenticar los usuarios. |

Para modificar los detalles del puerto, consulte "Modifique los hosts de plugins".

## Licencias SnapCenter

SnapCenter requiere varias licencias para permitir la protección de datos de aplicaciones, bases de datos, sistemas de archivos y máquinas virtuales. El tipo de licencia de SnapCenter que instale dependerá del entorno de almacenamiento y de las funciones que desee utilizar.

| Licencia | Donde se la requiere |
| --- | --- |
| Basado en controladora estándar de SnapCenter | Necesario para FAS y AFF<br><br>La licencia estándar de SnapCenter es una licencia basada en la controladora y se incluye como parte del paquete Premium. Si tiene la licencia de conjunto de SnapManager, también obtendrá el derecho de licencia estándar de SnapCenter. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS o AFF, puede obtener una licencia de evaluación Premium Bundle poniéndose en contacto con el representante de ventas.<br><br>SnapCenter también se ofrece como parte del paquete de protección de datos. Si ha adquirido el A400 o una versión posterior, debe comprar el paquete de protección de datos. |

| Licencia | Donde se la requiere |
| --- | --- |
| SnapCenter basada en capacidad estándar | Necesario con ONTAP Select y Cloud Volumes ONTAP<br><br>Si es cliente de Cloud Volumes ONTAP o ONTAP Select, necesita adquirir una licencia basada en capacidad por TB en función de los datos gestionados por SnapCenter. De forma predeterminada, SnapCenter envía una licencia de prueba integrada basada en capacidad estándar de SnapCenter de 90 días y 100 TB. Si desea obtener más detalles, póngase en contacto con el representante de ventas. |
| SnapMirror o SnapVault | ONTAP<br><br>Se requieren licencias de SnapMirror o SnapVault si la replicación se habilita en SnapCenter. |
| SnapRestore | Necesario para restaurar y verificar backups.<br><br>En sistemas de almacenamiento principales<br><br>• Requerida en sistemas de destino de SnapVault para realizar la verificación remota y restaurar desde un backup<br>• Requerida en sistemas de destino de SnapMirror para realizar la verificación remota |
| FlexClone | Necesario para clonar bases de datos y operaciones de verificación.<br><br>En sistemas de almacenamiento principales y secundarios<br><br>• Requerida en sistemas de destino de SnapVault para crear clones a partir de un backup de almacén secundario<br>• Requerida en sistemas de destino de SnapMirror para crear clones a partir de un backup de SnapMirror secundario |

| Licencia | Donde se la requiere |
| --- | --- |
| Protocolos | • Licencia de iSCSI o FC para LUN<br>• Licencia de CIFS para recursos compartidos de SMB<br>• Licencia de NFS para VMDK de tipo NFS<br>• Licencia de iSCSI o FC para VMDK de tipo VMFS<br><br>Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible |
| Licencias estándar de SnapCenter (opcional) | Destinos secundarios<br><br>Se recomienda, pero no es obligatorio, añadir licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter están deshabilitadas en destinos secundarios, no puede usar SnapCenter para realizar un backup de los recursos en el destino secundario después de realizar una operación de conmutación al nodo de respaldo. Sin embargo, se requiere una licencia de FlexClone en destinos secundarios para realizar operaciones de clonado y verificación. |

Las licencias avanzada y SnapCenter de servicios de archivos NAS de SnapCenter quedaron obsoletas y ya no están disponibles.

Debe instalar una o más licencias de SnapCenter. Para obtener información acerca de cómo agregar licencias, consulte "Añada licencias estándar basadas en controladora de SnapCenter" o. "Añada licencias basadas en capacidad estándar de SnapCenter".

**Licencias de Single Mailbox Recovery (SMBR)**

Si utiliza el plugin de SnapCenter para Exchange para gestionar bases de datos de Microsoft Exchange Server y Single Mailbox Recovery (SMBR), necesita una licencia adicional para SMBR, la cual debe adquirirse por separado en función del buzón de usuario.

NetApp® Single Mailbox Recovery ha llegado al final de la disponibilidad (EOA) el 12 de mayo de 2023. Para obtener más información, consulte "CPC-00507". NetApp continuará prestando soporte a los clientes que hayan adquirido capacidad, mantenimiento y soporte de sus buzones mediante números de referencia de marketing introducidos el 24 de junio de 2020, durante el periodo de concesión de soporte.

Single Mailbox Recovery de NetApp es un producto de partner que proporciona Ontrack. Ontrack PowerControls ofrece capacidades similares a las de Single Mailbox Recovery de NetApp. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls desde Ontrack (hasta licensingteam@ontrack.com) para la recuperación

granular de buzones después de la fecha EOA del 12 de mayo de 2023.

## Métodos de autenticación para las credenciales

Las credenciales utilizan métodos de autenticación diferentes según la aplicación o el entorno. Las credenciales autentican a los usuarios para que puedan realizar operaciones de SnapCenter. Debe crear un conjunto de credenciales para instalar plugins y otros conjuntos para operaciones de protección de datos.

### Autenticación de Windows

El método de autenticación de Windows autentica de acuerdo con Active Directory. Para la autenticación de Windows, se configura Active Directory fuera de SnapCenter. SnapCenter autentica sin configuración adicional. Se necesita una credencial de Windows para realizar ciertas tareas, como añadir hosts, instalar paquetes de plugins y programar trabajos.

### Autenticación de dominio que no es de confianza

SnapCenter permite la creación de credenciales de Windows mediante usuarios y grupos que pertenecen a dominios que no son de confianza. Para que la autenticación se complete correctamente, debe registrar los dominios que no son de confianza en SnapCenter.

### Autenticación de grupo de trabajo local

SnapCenter permite la creación de credenciales de Windows con grupos y usuarios de grupo de trabajo local. La autenticación de Windows para usuarios y grupos de grupos de trabajo locales no ocurre en el momento de la creación de credenciales de Windows, sino que se aplaza hasta que se realizan el registro de host y otras operaciones de host.

### Autenticación de SQL Server

El método de autenticación de SQL se verifica de acuerdo con una instancia de SQL Server. Esto significa que debe detectarse una instancia de SQL Server en SnapCenter. Por lo tanto, antes de añadir una credencial de SQL, debe añadir un host, instalar paquetes de plugins y actualizar los recursos. Necesita la autenticación de SQL Server para realizar operaciones, como programar en SQL Server o detectar recursos.

### Autenticación de Linux

El método de autenticación de Linux autentica con un host Linux. Necesita la autenticación de Linux durante el paso inicial de añadir el host Linux e instalar el paquete de plugins de SnapCenter para Linux de forma remota desde la interfaz gráfica de usuario de SnapCenter.

### Autenticación AIX

El método de autenticación AIX autentica con un host AIX. Necesita la autenticación de AIX durante el paso inicial de añadir el host AIX e instalar el paquete de plugins de SnapCenter para AIX de forma remota desde la interfaz gráfica de usuario de SnapCenter.

### Autenticación de base de datos de Oracle

El método de autenticación de base de datos de Oracle autentica con una base de datos de Oracle. Necesita una autenticación de base de datos de Oracle para realizar operaciones en la base de datos de Oracle si la autenticación de sistema operativo (SO) está deshabilitada en el host de bases de datos. Por lo tanto, antes

de agregar una credencial de base de datos Oracle, debe crear un usuario de Oracle en la base de datos Oracle con privilegios sysdba.

**Autenticación de Oracle ASM**

El método de autenticación de Oracle ASM autentica con una instancia de Oracle Automatic Storage Management (ASM). Si debe acceder a la instancia de Oracle ASM y si la autenticación de sistema operativo (SO) está deshabilitada en el host de bases de datos, se necesita una autenticación de Oracle ASM. Por lo tanto, antes de añadir una credencial de Oracle ASM, debe crear un usuario de Oracle con privilegios sysasm en la instancia de ASM.

**Autenticación de catálogo de RMAN**

El método de autenticación de catálogo de RMAN autentica con la base de datos de catálogos de Oracle Recovery Manager (RMAN). Si configuró un mecanismo de catálogo externo y registró la base de datos en la base de datos de catálogos, debe añadir una autenticación de catálogo de RMAN.

## Conexiones de almacenamiento y credenciales

Antes de ejecutar operaciones de protección de datos, debe configurar las conexiones de almacenamiento y añadir las credenciales que utilizarán SnapCenter Server y los plugins de SnapCenter.

- **Conexiones de almacenamiento**

  Las conexiones de almacenamiento conceden a SnapCenter Server y a los plugins de SnapCenter acceso al almacenamiento de ONTAP. La configuración de estas conexiones también implica la configuración de las funciones AutoSupport y del sistema de gestión de eventos (EMS).

- **Credenciales**

  - Administrador de dominio o cualquier miembro del grupo de administradores

    Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:

    - *NetBIOS\Username*
    - *Domain FQDN\Username*
    - *Username@upn*
  - Administrador local (sólo para grupos de trabajo)

    Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host.

  El formato válido para el campo Username es: *Username*

  - Credenciales para grupos de recursos individuales

    Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y

backup al nombre de usuario.

# Instale el servidor SnapCenter

## Puede ejecutar el ejecutable del instalador del servidor SnapCenter para instalar el servidor SnapCenter.

De forma opcional, puede ejecutar diversos procedimientos de instalación y configuración mediante cmdlets de PowerShell.

No se admite la instalación silenciosa del servidor SnapCenter desde la línea de comandos.

**Lo que necesitará**

- El host de SnapCenter Server debe estar actualizado con las actualizaciones de Windows y no tener reinicios del sistema pendientes.
- Debe haberse asegurado de que no está instalado MySQL Server en el host en el que planea instalar SnapCenter Server.
- Debe haber habilitado la depuración del instalador de Windows.

  Consulte el sitio Web de Microsoft para obtener información acerca de cómo habilitar "Registro del instalador de Windows".

  No debe instalar el servidor SnapCenter en un host que tenga servidores Microsoft Exchange Server, Active Directory o de nombres de dominio.

- Pasos*

1. Descargue el paquete de instalación del servidor SnapCenter desde "Sitio de soporte de NetApp".
2. Inicie la instalación del servidor SnapCenter haciendo doble clic en el archivo .exe descargado.

   Tras iniciar la instalación, se realizan todas las comprobaciones previas y si los requisitos mínimos no son los correctos, se muestran mensajes de error o de advertencia.

   Puede ignorar los mensajes de advertencia y continuar con la instalación; sin embargo, los errores deben corregirse.

3. Revise los valores rellenados previamente necesarios para la instalación del servidor SnapCenter y modifíquelos si es necesario.

   No es necesario especificar la contraseña para la base de datos de repositorio del servidor MySQL. Durante la instalación del servidor SnapCenter, la contraseña se genera automáticamente.

   El carácter especial "`"%" is not supported in the custom path for the repository database. If you include "%"`" en la ruta, la instalación falla.

4. Haga clic en **instalar ahora**.

   Si ha especificado valores que no son válidos, se mostrarán los mensajes de error adecuados. Debe volver a introducir los valores e iniciar la instalación.

Si hace clic en el botón **Cancelar**, se completará el paso que se está ejecutando y, a continuación, se iniciará la operación de reversión. El servidor SnapCenter se eliminará por completo del host.

Sin embargo, si hace clic en **Cancelar** cuando se están realizando las operaciones "reinicio del sitio del servidor SnapCenter" o "esperando inicio del servidor SnapCenter", la instalación continuará sin cancelar la operación.

Los archivos de registro siempre aparecen (los más antiguos primero) en la carpeta %temp% del usuario administrador. Si desea redirigir las ubicaciones de registro, inicie la instalación del servidor SnapCenter desde el símbolo del sistema ejecutando:`C:\installer_location\installer_name.exe /log"C:\"`

# Inicie sesión en SnapCenter

SnapCenter admite el control de acceso basado en roles (RBAC). El administrador de SnapCenter asigna roles y recursos a través del control de acceso basado en roles de SnapCenter a un usuario en un grupo de trabajo o directorio activo, o a grupos en Active Directory. El usuario de RBAC ahora puede iniciar sesión en SnapCenter con los roles asignados.

### Lo que necesitará

- Debe habilitar el servicio de activación de procesos de Windows (WAS) en Windows Server Manager.
- Si desea utilizar Internet Explorer como explorador para iniciar sesión en el servidor SnapCenter, debe asegurarse de que el modo protegido de Internet Explorer está deshabilitado.

### Acerca de esta tarea

Durante la instalación, el asistente de instalación del servidor de SnapCenter crea un acceso directo y lo coloca en el escritorio y en el menú Inicio del host donde está instalado SnapCenter. Además, al finalizar la instalación, el asistente de instalación muestra la URL de SnapCenter a partir de la información proporcionada durante la instalación, la cual se puede copiar para iniciar sesión desde un sistema remoto.

Si tiene varias pestañas abiertas en el navegador web, cerrar la pestaña del navegador SnapCenter no cierra la sesión de SnapCenter. Para finalizar la conexión con SnapCenter, debe cerrar la sesión de SnapCenter haciendo clic en el botón **Cerrar sesión** o cerrando todo el explorador web.

**Mejor práctica:** por razones de seguridad, se recomienda que no habilite su navegador para guardar su contraseña de SnapCenter.

La dirección URL predeterminada de la interfaz gráfica de usuario es una conexión segura con el puerto 8146 predeterminado en el servidor donde está instalado el servidor SnapCenter (*https://server:8146*). Si se proporcionó un puerto un puerto diferente durante la instalación de SnapCenter, se usa ese puerto.

Para la implementación de alta disponibilidad (ha), debe acceder a SnapCenter mediante la IP del clúster virtual *https://Virtual_Cluster_IP_or_FQDN:8146*. Si no ve la interfaz de usuario de SnapCenter al ir a *https://Virtual_Cluster_IP_or_FQDN:8146* en Internet Explorer (IE), debe añadir la dirección IP de clúster virtual o FQDN como un sitio de confianza de IE en cada host de plugin. Otra opción es deshabilitar la

seguridad mejorada de IE en cada host del plugin. Para obtener más información, consulte "No se puede acceder a la dirección IP del clúster desde la red externa".

Además de usar la interfaz gráfica de usuario de SnapCenter, es posible usar los cmdlets de PowerShell para crear scripts para llevar a cabo operaciones de configuración, backup y restauración. Es posible que algunos cmdlets se hayan modificado en cada versión de SnapCenter. La "Guía de referencia de cmdlets de SnapCenter Software" tiene los detalles.

Si es la primera vez que inicia sesión en SnapCenter, debe usar las credenciales que proporcionó durante el proceso de instalación.

- Pasos*

1. Inicie SnapCenter desde el acceso directo creado en el escritorio de host local, o desde la URL provista al final de la instalación o desde la URL que proporcionó el administrador de SnapCenter.
2. Introduzca las credenciales de usuario.

| Para especificar lo siguiente… | Utilice uno de estos formatos… |
|---|---|
| Administrador del dominio | • NetBIOS\Username<br>• Sufijo Username@UPN<br>Por ejemplo, username@netapp.com<br>• El dominio FQDN\Username |
| Administrador local | Nombre de usuario |

3. Si tiene asignado más de un rol, en el recuadro Role seleccione el rol que desea usar para esta sesión de inicio.

   Su usuario actual y el rol asociado se muestran en la esquina superior derecha de SnapCenter después de iniciar sesión.

**Resultados**

Aparece la página **Panel**.

Si se produce un error en el registro y no se puede acceder al sitio, debe asignar el certificado SSL a SnapCenter. "Leer más"

**Después de terminar**

Después de iniciar sesión en SnapCenter Server como usuario con RBAC por primera vez, actualice la lista de recursos.

Si tiene dominios de Active Directory que no son de confianza y desea que SnapCenter admita, debe registrar esos dominios con SnapCenter antes de configurar las funciones para los usuarios en dominios que no son de confianza. "Leer más"

## Modifique el tiempo de espera de sesión de interfaz gráfica de usuario predeterminada de SnapCenter

Puede modificar el tiempo de espera de sesión de la interfaz gráfica de usuario de SnapCenter de modo que sea inferior o superior al tiempo de espera predeterminado de 20 minutos.

Como función de seguridad, después de un tiempo predeterminado de 15 minutos de inactividad, SnapCenter le advertirá de que se cerrará sesión en la sesión de la interfaz gráfica de usuario en 5 minutos. De forma predeterminada, SnapCenter cierra la sesión de la interfaz gráfica de usuario tras 20 minutos de inactividad, de modo que deberá iniciar sesión de nuevo.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Configuración** > **Configuración global**.
  2. En la página Global Settings, haga clic en **Configuración**.
  3. En el campo tiempo de espera de la sesión, introduzca el nuevo tiempo de espera de la sesión en minutos y, a continuación, haga clic en **Guardar**.

## Proteja el servidor web de SnapCenter mediante la desactivación de SSL 3.0

Por motivos de seguridad, debería deshabilitar el protocolo de capa de sockets seguros (SSL) 3.0 en Microsoft IIS si está activado en el servidor web de SnapCenter.

Existen defectos en el protocolo SSL 3.0 que un atacante puede utilizar para provocar fallos de conexión o para realizar ataques de tipo "man in the middle" y observar el tráfico de cifrado entre su sitio web y sus visitantes.

- Pasos*
  1. Para iniciar el Editor del Registro en el host del servidor web SnapCenter, haga clic en **Inicio** > **Ejecutar** y, a continuación, escriba regedit.
  2. En el Editor del Registro, desplácese hasta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
     - Si la clave del servidor ya existe:
       i. Seleccione el DWORD activado y, a continuación, haga clic en **Editar** > **Modificar**.
       ii. Cambie el valor a 0 y, a continuación, haga clic en **Aceptar**.
     - Si la clave del servidor no existe:
       i. Haga clic en **Editar** > **Nuevo** > **clave** y, a continuación, asigne un nombre al servidor de claves.
       ii. Con la nueva clave de servidor seleccionada, haga clic en **Edición** > **Nuevo** > **DWORD**.
       iii. Asigne un nombre al nuevo DWORD activado y, a continuación, introduzca 0 como el valor.
  3. Cierre el Editor del Registro.

# Configurar certificado de CA

## Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado

que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

> Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

## Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

- Pasos*

1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
2. En la ventana **Agregar o quitar complementos**, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
3. En la ventana del complemento **certificados**, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
|---|---|
| Importar clave privada | Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**. |
| Importar formato de archivo | No realice cambios; haga clic en **Siguiente**. |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |

| En esta ventana del asistente… | Haga lo siguiente… |
| --- | --- |
| Finalización del Asistente para importación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación. |

El certificado de importación debe incluirse con la clave privada (los formatos admitidos son: *.pfx, *.p12, *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

## Obtenga la huella digital del certificado de CA

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

- Pasos*

1. Realice lo siguiente en la interfaz gráfica de usuario:
   a. Haga doble clic en el certificado.
   b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
   c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
   d. Copie los caracteres hexadecimales del cuadro.
   e. Quite los espacios entre los números hexadecimales.

      Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:
   a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

      *Get-ChildItem -Path Cert:\LocalMachine\My*

   b. Copie la huella digital.

## Configure el certificado de CA con servicios de plugins de host de Windows

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

- Pasos*

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

Por ejemplo:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Enlace el certificado recientemente instalado con los servicios de
plugins del host de Windows mediante la ejecución de los siguientes
comandos:
```

```
> $cert = "<certificate thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
```

Por ejemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

## Configurar el certificado de CA con el sitio SnapCenter

Debe configurar el certificado de CA con el sitio SnapCenter en el host de Windows.

- Pasos*
  1. Abra el Administrador de IIS en el servidor de Windows donde está instalado SnapCenter.
  2. En el panel de navegación izquierdo, haga clic en **conexiones**.
  3. Expanda el nombre del servidor y **Sitios**.
  4. Seleccione el sitio web de SnapCenter en el que desea instalar el certificado SSL.
  5. Vaya a **acciones** > **Editar sitio**, haga clic en **Enlaces**.
  6. En la página vinculaciones, seleccione **enlace para https**.
  7. Haga clic en **Editar**.
  8. En la lista desplegable Certificado SSL, seleccione el Certificado SSL importado recientemente.
  9. Haga clic en **Aceptar**.

Si el certificado de CA implementado recientemente no aparece en el menú desplegable, compruebe si el certificado de CA está asociado a la clave privada.

Asegúrese de que el certificado se agregue mediante la siguiente ruta: **Raíz de consola > certificados – Equipo local > entidades de certificación raíz de confianza > certificados**.

### Habilite los certificados de CA para SnapCenter

Debe configurar los certificados de CA y habilitar la validación de certificados de CA para el servidor SnapCenter.

**Lo que necesitará**

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet Set-SmCertificateSettings.
- Puede mostrar el estado del certificado del servidor SnapCenter mediante el cmdlet de Get-SmCertificateSettings.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En la página Configuración, vaya a **Configuración** > **Configuración global** > **Configuración del certificado CA**.
  2. Seleccione **Activar validación de certificados**.
  3. Haga clic en **aplicar**.

**Después de terminar**

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que no hay ningún certificado de CA habilitado o asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

# Registrar dominios de Active Directory que no son de confianza

Debe registrar Active Directory en el servidor de SnapCenter para administrar hosts, usuarios y grupos de varios dominios de Active Directory que no son de confianza.

**Lo que necesitará**

- Se debe acceder al nombre de dominio completo (FQDN) desde SnapCenter Server.
- Si el FQDN no se puede resolver, las direcciones IP de las controladoras de dominio proporcionadas deben poder resolverse de SnapCenter Server.
- Debe haber habilitado la comunicación bidireccional entre los hosts del plugin y SnapCenter Server.
- La resolución de DNS se debe configurar desde el servidor de SnapCenter a los hosts del plugin y viceversa.

**Acerca de esta tarea**

Puede registrar un dominio no confiable con el FQDN. Si el FQDN no se puede resolver desde el servidor SnapCenter, puede registrarse con una dirección IP.

Puede utilizar la interfaz de usuario de SnapCenter o los cmdlets de PowerShell para registrar un dominio que no es de confianza.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Configuración global**.
  3. En la página Global Settings (Configuración global), haga clic en **Configuración de dominio**.
  4. Haga clic en + para registrar un nuevo dominio.
  5. En la página Registrar nuevo dominio, especifique la información necesaria para registrar el dominio que no es de confianza:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Nombre de dominio | Especifique el nombre NetBIOS para el dominio. |
| Dominio FQDN | Especifique el FQDN y haga clic en **resolver**. |
| Direcciones IP del controlador de dominio | Si el dominio FQDN no se puede resolver desde el servidor SnapCenter, especifique una o más direcciones IP de las controladoras de dominio.<br><br>Para obtener más información, consulte "Agregue la IP del controlador de dominio para dominios que no sean de confianza desde la interfaz gráfica de usuario". |

  6. Haga clic en **Aceptar**.

# Configuración de la alta disponibilidad

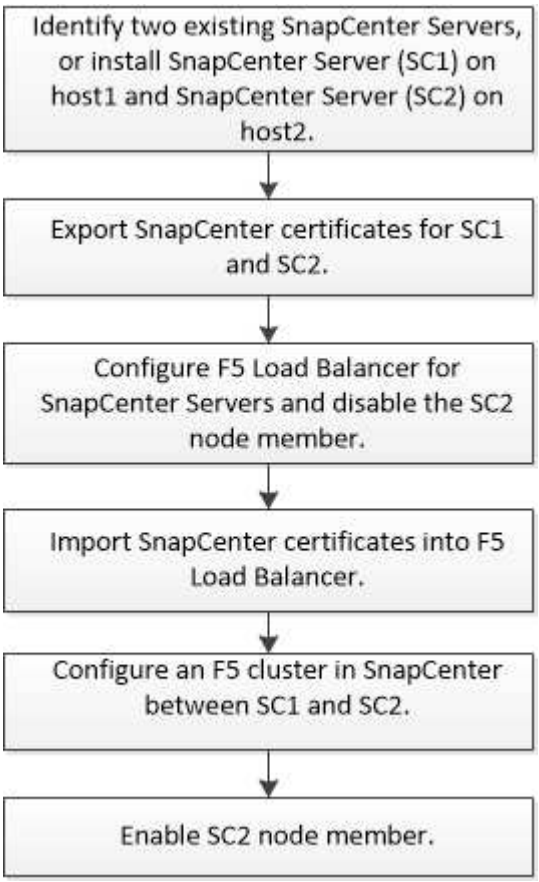
## Configurar servidores SnapCenter para alta disponibilidad mediante F5

Para admitir la alta disponibilidad (ha) en SnapCenter, puede instalar el equilibrador de carga F5. F5 permite al servidor SnapCenter admitir configuraciones activo-pasivo en hasta dos hosts que se encuentran en la misma ubicación. Para utilizar el equilibrador de carga F5 en SnapCenter, debe configurar SnapCenter Server y el equilibrador de carga F5.

Si ha actualizado desde SnapCenter 4.2.x y anteriormente utilizaba balanceo de carga de red (NLB), puede continuar utilizando dicha configuración o cambiar a F5.

La imagen del flujo de trabajo enumera los pasos para configurar SnapCenter Server para una alta

disponibilidad utilizando el equilibrador de carga F5. Para obtener instrucciones detalladas, consulte "Cómo configurar instancias de SnapCenter Server para obtener una alta disponibilidad mediante el balanceador de carga F5".




Debe ser miembro del grupo de administradores locales en SnapCenter Server (además de tener la asignación del rol de administrador de SnapCenter) para usar los siguientes cmdlets con el fin de agregar y quitar clústeres de F5:

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  Para obtener más información, consulte "Guía de referencia de cmdlets de SnapCenter Software".

#### Información de configuración adicional de F5

- Después de instalar y configurar SnapCenter para alta disponibilidad, edite el acceso directo del escritorio de SnapCenter para que apunte a la IP del clúster de F5.
- Si se produce una conmutación por error entre los servidores SnapCenter y existe también una sesión SnapCenter, debe cerrar el explorador e iniciar sesión en SnapCenter de nuevo.
- En la configuración del equilibrador de carga (NLB o F5), si agrega un nodo que se resuelve parcialmente mediante el nodo NLB o F5, y si el nodo SnapCenter no puede conectarse a este nodo, la página de host de SnapCenter cambia entre los hosts a estado en ejecución con frecuencia. Para resolver este problema, debe asegurarse de que los dos nodos SnapCenter puedan resolver el host en el nodo NLB o F5.

## Configure el balanceador de carga de red de Microsoft manualmente

Es posible configurar el balanceo de carga de red de Microsoft (NLB) para configurar la función de alta disponibilidad de SnapCenter. En SnapCenter 4.2, debe configurar manualmente NLB fuera de la instalación de SnapCenter para obtener alta disponibilidad.

Para obtener más información acerca de cómo configurar el balanceo de carga de red (NLB) con SnapCenter, consulte "Cómo configurar NLB con SnapCenter".

SnapCenter 4.1.1 o una configuración compatible con una versión anterior de balanceo de carga de red (NLB) al instalar SnapCenter.

## Cambie de NLB a F5 para ofrecer alta disponibilidad

Es posible cambiar la configuración de alta disponibilidad de SnapCenter de balanceo de carga de red (NLB) para usar el balanceador de carga F5.

- Pasos*
  1. Configurar servidores SnapCenter para obtener alta disponibilidad mediante F5. "Leer más".
  2. En el host de SnapCenter Server, inicie PowerShell.
  3. Inicie una sesión con el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
  4. Actualice el servidor SnapCenter para que apunte a la dirección IP del clúster F5 mediante el cmdlet Update-SmServerCluster.

     La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Alta disponibilidad del repositorio MySQL de SnapCenter

La replicación de MySQL es una de las características de MySQL Server que permite replicar datos de un servidor de bases de datos de MySQL (maestro) a otro servidor de bases de datos de MySQL (esclavo). SnapCenter admite la replicación de MySQL para alta disponibilidad solamente en dos nodos habilitados para el balanceo de carga de red (NLB, Network Load Balancing).

SnapCenter ejecuta operaciones de lectura o escritura en el repositorio maestro y enruta su conexión hacia el repositorio esclavo cuando se produce un fallo en el repositorio maestro. En ese caso, el repositorio esclavo se convierte en repositorio maestro. SnapCenter también admite la replicación en sentido inverso, que se habilita únicamente en casos de conmutación por error.

Si desea usar la función de alta disponibilidad de MySQL, debe configurar Network Load Balancer (NLB) en el primer nodo. El repositorio de MySQL se instala en este nodo, como parte integral de la propia instalación. Al instalar SnapCenter en el segundo nodo, debe unirlo al F5 del primer nodo y crear una copia del repositorio de MySQL en el segundo nodo.

SnapCenter proporciona los cmdlets de *Get-SmRepositoryConfig* y *Set-SmRepositoryConfig* PowerShell para gestionar la replicación de MySQL.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Debe tener en cuenta las limitaciones relacionadas con la función de alta disponibilidad de MySQL:

- El balanceo de carga de red y la alta disponibilidad de MySQL tan solo se admiten en dos nodos.
- No es posible conmutar y cambiar de una instalación independiente de SnapCenter a una instalación con balanceo de carga de red o viceversa ni hacerlo de una configuración independiente de MySQL a una configuración de alta disponibilidad de MySQL.
- La función de conmutación automática por error no es viable si los datos del repositorio esclavo no están sincronizados con los datos del repositorio maestro.

  Puede iniciar una conmutación por error forzada con ayuda del cmdlet *Set-SmRepositoryConfig*.

- Cuando se inicia la conmutación por error, los trabajos que estén ejecutándose pueden sufrir errores.

  Si se produce una conmutación por error debida a que MySQL Server o SnapCenter Server están inoperativos, cualquiera de los trabajos que estén ejecutándose podría fallar. Después de producirse un error y conmutar al segundo nodo, todos los siguientes trabajos se ejecutarán correctamente.

Para obtener información acerca de cómo configurar la alta disponibilidad, consulte "Cómo configurar NLB y ARR con SnapCenter".

## Exportar certificados SnapCenter

- Pasos*

  1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar complemento**.
  2. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
  3. En la ventana del complemento certificados, seleccione la opción **Mi cuenta de usuario** y, a continuación, haga clic en **Finalizar**.
  4. Haga clic en **raíz de consola** > **certificados - Usuario actual** > **entidades de certificación raíz de confianza** > **certificados**.
  5. Haga clic con el botón derecho del ratón en el certificado que tiene el nombre descriptivo de SnapCenter y, a continuación, seleccione **todas las tareas** > **Exportar** para iniciar el asistente de exportación.
  6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
|---|---|
| Exportar clave privada | Seleccione la opción **Sí, exporte la clave privada** y, a continuación, haga clic en **Siguiente**. |
| Exportar formato de archivo | No realice cambios; haga clic en **Siguiente**. |

| En esta ventana del asistente… | Haga lo siguiente… |
| --- | --- |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |
| Archivo a exportar | Especifique un nombre de archivo para el certificado exportado (debe utilizar .pfx) y, a continuación, haga clic en **Siguiente**. |
| Finalización del Asistente para exportación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la exportación. |

**Resultados**

Los certificados se exportan en formato .pfx.

# Configurar el control de acceso basado en roles (RBAC)

## Añada un usuario o grupo y asigne roles y activos

Para configurar el control de acceso basado en roles para usuarios de SnapCenter, es posible añadir usuarios o grupos y asignar roles. El rol determina las opciones a las que los usuarios de SnapCenter pueden acceder.

**Lo que necesitará**

- Inició sesión con el rol de administrador de SnapCenter.
- Creó las cuentas de usuario o de grupo en Active Directory mediante el sistema operativo o la base de datos. No se puede usar SnapCenter para crear estas cuentas.

  Los nombres de usuario y de grupo no deben incluir los caracteres /\[ ];|=,+*?< >'.

- SnapCenter incluye varios roles predefinidos.

  Es posible asignar estos roles al usuario o crear roles nuevos.

- Los usuarios DE AD y los grupos de AD que se agregan al control de acceso basado en roles de SnapCenter deben tener el permiso DE LECTURA en el contenedor usuarios y en el contenedor equipos de Active Directory.
- Después de asignar un rol a un usuario o grupo que contiene los permisos correspondientes, debe asignar el acceso de usuario a activos de SnapCenter, como hosts y conexiones de almacenamiento.

  De este modo, los usuarios pueden realizar las acciones para las cuales tienen permisos sobre los activos que les asignaron.

- Es necesario asignar un rol al usuario o grupo en algún momento para aprovechar los permisos y las eficiencias de RBAC.
- Puede asignar activos como host, grupos de recursos, políticas, conexión de almacenamiento, plugin, y

las credenciales para el usuario mientras crea el usuario o el grupo.

- Los activos mínimos que debe asignar un usuario para realizar ciertas operaciones son los siguientes:

| Funcionamiento | Asignación de activos |
|---|---|
| Proteja los recursos | host, política |
| Backup | host, grupo de recursos, política |
| Restaurar | host, grupo de recursos |
| Clonar | host, grupo de recursos, política |
| Ciclo de vida de clon | host |
| Cree un grupo de recursos | host |

- Cuando se agrega un nodo nuevo a un clúster de Windows o a un activo DAG (Grupo de disponibilidad de base de datos de Exchange Server) y si este nodo nuevo se asigna a un usuario, debe reasignar el activo al usuario o grupo para incluir el nodo nuevo al usuario o grupo.

  Debe reasignar el usuario o el grupo de RBAC al clúster o DAG para incluir el nodo nuevo al usuario o grupo de RBAC. Por ejemplo, tiene un clúster de dos nodos y ha asignado un usuario o un grupo RBAC al clúster. Cuando añada otro nodo al clúster, debe reasignar al usuario o grupo de RBAC al clúster para incluir el nodo nuevo del usuario o grupo de RBAC.

- Si tiene pensado replicar copias de Snapshot, la conexión de almacenamiento tanto para el volumen de origen como de destino debe asignarse al usuario que realiza la operación.

  Antes de asignar acceso a los usuarios, debería añadir activos.

Si utiliza las funciones del plugin de SnapCenter para VMware vSphere para proteger máquinas virtuales, VMDK o almacenes de datos, debe utilizar la interfaz gráfica de usuario de VMware vSphere para añadir un usuario de vCenter a un rol del plugin de SnapCenter para VMware vSphere. Para obtener más información sobre los roles de VMware vSphere, consulte "Roles predefinidos del plugin de SnapCenter para VMware vSphere".

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **usuarios y acceso** > .
  3. En la página Agregar usuarios/grupos desde Active Directory o Workgroup:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de acceso | Seleccione dominio o grupo de trabajo<br><br>Para el tipo de autenticación de dominio, debe especificar el nombre de dominio del usuario o grupo al que desea añadir el usuario a un rol.<br><br>De forma predeterminada, se completa automáticamente con el nombre de dominio que ha iniciado sesión.<br><br>Debe registrar el dominio que no es de confianza en la página **Configuración** > **Configuración global** > **Configuración de dominio**. |
| Tipo | Seleccione User o Group<br><br>SnapCenter solo admite el grupo de seguridad y no el grupo de distribución. |
| Nombre de usuario | a. Escriba el nombre de usuario parcial y, a continuación, haga clic en **Agregar**.<br><br>El nombre de usuario distingue entre mayúsculas y minúsculas.<br><br>b. Seleccione el nombre de usuario en la lista de búsqueda.<br><br>Cuando agrega usuarios de un dominio diferente o de un dominio que no es de confianza, debe escribir el nombre de usuario completamente porque no hay lista de búsqueda para usuarios de varios dominios.<br><br>Repita este paso para añadir usuarios o grupos adicionales al rol seleccionado. |
| Funciones | Seleccione el rol al que desea añadir el usuario. |

4. Haga clic en **asignar** y, a continuación, en la página asignar activos:
   a. Seleccione el tipo de activo en la lista desplegable **activo**.

b. En la tabla Asset, seleccione el activo.

   Los activos solo aparecen si el usuario ha añadido los activos a SnapCenter.

c. Repita este procedimiento para todos los activos necesarios.

d. Haga clic en **Guardar**.

5. Haga clic en **Enviar**.

   Después de agregar usuarios o grupos y asignar roles, actualice la lista de recursos.

## Crear un rol

Además de usar los roles de SnapCenter existentes, es posible crear roles propios y personalizar los permisos.

Inició sesión con el rol de administrador de SnapCenter.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **roles**.
3. Haga clic en .
4. En la página Add Role, especifique un nombre y una descripción para el nuevo rol.

   En SnapCenter 4.5, no puede tener un nombre de rol que incluya los caracteres /\[ ];|=,+*?< >'. Si desea utilizar una función creada en una versión anterior de SnapCenter con estos caracteres especiales, puede deshabilitar la validación del nombre de la función cambiando el valor del parámetro 'DisableSQLInjtionValidation' a TRUE.

5. Seleccione **todos los miembros de esta función pueden ver los objetos de otros miembros** para permitir que otros miembros de la función vean recursos como volúmenes y hosts después de actualizar la lista de recursos.

   Debe anular la selección de esta opción si no desea que los miembros del rol vean los objetos a los que se asignaron otros miembros.

   Cuando se habilita esta opción, no es necesario asignar a los usuarios acceso a los objetos o recursos si los usuarios pertenecen al mismo rol que el usuario que creó los objetos o recursos.

1. En la página permisos, seleccione los permisos que desea asignar a la función o haga clic en **Seleccionar todo** para conceder todos los permisos a la función.
2. Haga clic en **Enviar**.

## Añadir un rol de RBAC de ONTAP mediante comandos de inicio de sesión de seguridad

Puede utilizar los comandos Security login para añadir un rol de RBAC de ONTAP si los sistemas de almacenamiento ejecutan ONTAP almacenado en clúster.

**Lo que necesitará**

- Antes de crear un rol de RBAC de ONTAP para sistemas de almacenamiento que ejecutan ONTAP almacenado en clúster, debe identificar los siguientes aspectos:
  - La tarea (o las tareas) que desee ejecutar
  - Los privilegios necesarios para ejecutar esas tareas
- Para configurar un rol de RBAC es necesario que lleve a cabo las siguientes acciones:
  - Conceda privilegios a comandos o directorios de comandos.

    Hay dos niveles de acceso para cada directorio de comandos/comandos: Acceso total y sólo lectura.

  Siempre debe asignar los privilegios de acceso total en primer lugar.

  - Asigne roles a los usuarios.
  - Varíe su configuración según si los plugins de SnapCenter están conectados a la IP de administrador del clúster para todo el clúster en conjunto o están directamente conectados a una máquina virtual SVM dentro del clúster.

**Acerca de esta tarea**

Para simplificar la configuración de estos roles en los sistemas de almacenamiento, puede utilizar la herramienta RBAC User Creator for Data ONTAP, que se encuentra en el foro de comunidades de NetApp.

Esta herramienta se encarga automáticamente de configurar los privilegios de ONTAP correctamente. Por ejemplo, la herramienta RBAC User Creator for Data ONTAP agrega automáticamente los privilegios en el orden correcto, para que los privilegios de acceso total aparezcan primero. Si añade primero los privilegios solo de lectura y después añade los privilegios de acceso total, ONTAP Marca los privilegios de acceso total como duplicados y los omite.

> Si posteriormente actualiza SnapCenter u ONTAP, debe volver a ejecutar la herramienta RBAC User Creator for Data ONTAP para actualizar los roles de usuario que ha creado previamente. Los roles de usuario creados para una versión anterior de SnapCenter o ONTAP no funcionan correctamente con las versiones actualizadas. Cuando vuelva a ejecutar la herramienta, automáticamente se encarga de la actualización. No es necesario que vuelva a recrear los roles.

Más información sobre la configuración de roles de RBAC de ONTAP, consulte "Guía completa de autenticación de administrador y RBAC de ONTAP 9".

> Para salvaguardar la consistencia, la documentación de SnapCenter se refiere a los roles como funciones que usan privilegios. La GUI de System Manager de OnCommand utiliza el término «'atributo» en lugar de «'privilegio». Al configurar roles de RBAC de ONTAP, ambos términos significan lo mismo.

- Pasos*

1. En el sistema de almacenamiento, introduzca el comando siguiente para crear un rol nuevo:

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

- svm_name es el nombre de la máquina virtual SVM. Si deja este espacio en blanco, se tomará de forma predeterminada el administrador del clúster.
- role_name es el nombre que usted especifica para el rol.
- Command es la capacidad de ONTAP.

> Debe repetir este comando para cada permiso. Recuerde que los comandos de acceso total deben enumerarse antes que los comandos de solo lectura.

Para obtener más información sobre la lista de permisos, consulte "Comandos de la CLI de ONTAP para crear roles y asignar permisos".

2. Cree un nombre de usuario introduciendo el comando siguiente:

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

- user_name es el nombre de usuario que va a crear.
- <password> es su contraseña. Si no especifica una contraseña, el sistema le solicitará una.
- svm_name es el nombre de la máquina virtual SVM.

3. Para asignar el rol al usuario, introduzca el siguiente comando:

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

- <user_name> es el nombre del usuario que creó en el paso 2. Este comando permite que usted modifique el usuario para asociarlo al rol.
- <svm_name> es el nombre de la SVM.
- <role_name> es el nombre del rol que creó en el paso 1.
- <password> es su contraseña. Si no especifica una contraseña, el sistema le solicitará una.

4. Compruebe que el usuario se ha creado correctamente introduciendo el comando siguiente:

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

User_name es el nombre del usuario que creó en el Paso 3.

## Cree roles de SVM con privilegios mínimos

Hay varios comandos de la CLI de ONTAP que debe ejecutar cuando crea un rol para un usuario de SVM nuevo en ONTAP. Este rol es obligatorio si configura SVM en ONTAP para su uso con SnapCenter y no desea utilizar el rol vsadmin.

- Pasos*

1. En el sistema de almacenamiento, cree un rol y asigne todos los permisos al rol.

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

```
-cmddirname <permission\>
```

Debe repetir este comando para cada permiso.

1. Cree un usuario y asigne el rol a ese usuario.

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

2. Desbloquee el usuario.

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

### Comandos de la CLI de ONTAP para crear roles de SVM y asignar permisos

Hay varios comandos de la CLI de ONTAP que debe ejecutar para crear roles de SVM y asignar permisos.

- `security login role create -role SVM_SVM_Role_Name -cmddirname "snapmirror list-destinations" -vserver SVM_Name -access all`
- `security login role create -role SVM_SVM_Role_Name -cmddirname "event generate-autosupport-log" -vserver SVM_Name -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "lun mapping create" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"volume clone create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
  `*security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "volume clone split status" -access all`

### Cree roles de clúster ONTAP con privilegios mínimos

Debe crear un rol de clúster de ONTAP con privilegios mínimos para poder no usar el rol de administrador de ONTAP para realizar operaciones en SnapCenter. Es posible ejecutar varios comandos de la CLI de ONTAP para crear el rol del clúster de ONTAP y

asignar privilegios mínimos.

- Pasos*

1. En el sistema de almacenamiento, cree un rol y asigne todos los permisos al rol.

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

Debe repetir este comando para cada permiso.

1. Cree un usuario y asigne el rol a ese usuario.

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

2. Desbloquee el usuario.

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

**Comandos de la CLI de ONTAP para crear roles de clúster y asignar permisos**

Hay varios comandos de la CLI de ONTAP que debe ejecutarse para crear roles de clúster y asignar permisos.

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

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

"network interface create" -access readonly

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume qtree modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

## Configure los grupos de aplicaciones de IIS para habilitar los permisos de lectura de Active Directory

Puede configurar Servicios de Internet Information Server (IIS) en Windows Server para crear una cuenta personalizada del grupo de aplicaciones cuando necesite habilitar los permisos de lectura de Active Directory para SnapCenter.

- Pasos*
  1. Abra el Administrador de IIS en el servidor de Windows donde está instalado SnapCenter.
  2. En el panel de navegación izquierdo, haga clic en **grupos de aplicaciones**.
  3. Seleccione SnapCenter en la lista grupos de aplicaciones y, a continuación, haga clic en **Configuración avanzada** en el panel acciones.
  4. Seleccione identidad y, a continuación, haga clic en **…** para editar la identidad del grupo de aplicaciones SnapCenter.
  5. En el campo cuenta personalizada, introduzca un nombre de usuario de dominio o de administrador de dominio con permiso de lectura de Active Directory.

6. Haga clic en Aceptar.

   La cuenta personalizada reemplaza la cuenta de ApplicationPoolIdentity integrada para el grupo de aplicaciones de SnapCenter.

# Añadir sistemas de almacenamiento

## Debe configurar el sistema de almacenamiento que ofrezca acceso SnapCenter al almacenamiento de ONTAP o Amazon FSX para ONTAP de NetApp a fin de realizar operaciones de protección y aprovisionamiento de datos.

Puede añadir una SVM independiente o un clúster compuesto por múltiples SVM. Si utiliza Amazon FSX para ONTAP de NetApp, puede agregar la LIF de administrador de FSX compuesta por varias SVM mediante la cuenta fsxadmin en SnapCenter 4.5 P1 o agregar FSX SVM en SnapCenter.

**Lo que necesitará**

- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

  No debe haber instalaciones de complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

  SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de datos única.

**Acerca de esta tarea**

- Al configurar sistemas de almacenamiento, también es posible habilitar las funciones sistema de gestión de eventos (EMS) y AutoSupport. La herramienta AutoSupport recoge datos sobre el estado del sistema y los envía automáticamente al soporte técnico de NetApp para que el equipo pueda solucionar problemas en el sistema.

  Si se habilitan estas funciones, SnapCenter envía la información de AutoSupport al sistema de almacenamiento y mensajes de EMS al syslog del sistema de almacenamiento cuando se protege un recurso, una operación de restauración o clonado se completa correctamente o una operación genera errores.

- Si planifica replicar copias de Snapshot en un destino de SnapMirror o un destino de SnapVault, debe configurar conexiones al sistema de almacenamiento para la SVM o el clúster de destino, así como la SVM o el clúster de origen.

Si cambia la contraseña del sistema de almacenamiento, se pueden producir errores en las operaciones programadas, de backup bajo demanda y de restauración. Después de cambiar la contraseña del sistema de almacenamiento, puede actualizar la contraseña haciendo clic en **Modificar** en la ficha almacenamiento.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **sistemas de almacenamiento**.
  2. En la página Storage Systems, haga clic en **Nuevo**.
  3. En la página Add Storage System, proporcione la siguiente información:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Sistema de almacenamiento | Introduzca el nombre o la dirección IP del sistema de almacenamiento.<br><br>Los nombres de los sistemas de almacenamiento, sin incluir el nombre de dominio, deben tener 15 o menos caracteres y los nombres deben poder resolverse. Para crear conexiones del sistema de almacenamiento con nombres de más de 15 caracteres, se puede usar el cmdlet Add-SmStorageConnectionPowerShell.<br><br>En el caso de los sistemas de almacenamiento con configuración MetroCluster (MCC), se recomienda registrar tanto clústeres locales como de otros fabricantes para garantizar operaciones no disruptivas.<br><br>SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada una de las SVM que admite SnapCenter debe tener un nombre único.<br><br>Después de añadir la conexión de almacenamiento a SnapCenter, no debe cambiar el nombre de la SVM o el clúster mediante ONTAP.<br><br>Si se añade SVM con un nombre corto o FQDN, debe poder resolverse tanto del SnapCenter como del host del plugin. |
| Nombre de usuario/Contraseña | Introduzca las credenciales del usuario de almacenamiento que tenga los privilegios necesarios para acceder al sistema de almacenamiento. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Sistema de gestión de eventos (EMS) y configuración de AutoSupport | Si desea enviar mensajes de EMS al syslog del sistema de almacenamiento, o si desea que se envíen mensajes de AutoSupport al sistema de almacenamiento cuando se aplica la protección, se completan correctamente operaciones de restauración o se producen errores en las operaciones, seleccione la casilla de comprobación correspondiente.<br><br>Al seleccionar la casilla de verificación **Enviar notificación AutoSupport para operaciones con errores al sistema de almacenamiento**, también se selecciona la casilla de verificación **Registrar eventos del servidor SnapCenter a syslog** porque se requiere la mensajería EMS para habilitar las notificaciones AutoSupport. |

4. Haga clic en **más opciones** si desea modificar los valores predeterminados asignados a la plataforma, el protocolo, el puerto y el tiempo de espera.
   a. En Plataforma, seleccione una de las opciones de la lista desplegable.

      Si la SVM es el sistema de almacenamiento secundario en una relación de copia de seguridad, seleccione la casilla de verificación **Secundaria**. Cuando se selecciona la opción **secundario**, SnapCenter no realiza una comprobación de licencia inmediatamente.

   b. En Protocol, seleccione el protocolo que se configuró durante la configuración del SVM o el clúster, que suele ser HTTPS.
   c. Introduzca el puerto que acepta el sistema de almacenamiento.

      El puerto 443 predeterminado normalmente funciona.

   d. Introduzca el tiempo en segundos que debe transcurrir antes de que se interrumpan los intentos de comunicación.

      El valor predeterminado es 60 segundos.

   e. Si la SVM tiene varias interfaces de gestión, seleccione la casilla de comprobación **Preferred IP** y, a continuación, introduzca la dirección IP preferida para las conexiones con la SVM.
   f. Haga clic en **Guardar**.
5. Haga clic en **Enviar**.

**Resultados**

En la página Storage Systems, en el menú desplegable **Tipo** realice una de las siguientes acciones:

- Seleccione **ONTAP SVM** si desea ver todas las SVM que se han añadido.

  Si ha añadido SVM FSX, las SVM FSX aparecen aquí.

- Seleccione **clústeres ONTAP** si desea ver todos los clústeres que se han agregado.

Si ha agregado clústeres FSX utilizando fsxadmin, los clústeres FSX se enumeran aquí.

Cuando hace clic en el nombre del clúster, todas las SVM que forman parte del clúster se muestran en la sección Storage Virtual Machines.

Si se añade una nueva SVM al clúster de ONTAP mediante la GUI de ONTAP, haga clic en **Rediscover** para ver la SVM recién añadida.

**Después de terminar**

Un administrador de clúster debe habilitar AutoSupport en cada nodo del sistema de almacenamiento para enviar notificaciones por correo electrónico desde todos los sistemas de almacenamiento a los que tiene acceso SnapCenter. Para ello, ejecute el siguiente comando desde la línea de comandos del sistema de almacenamiento:

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

El administrador de máquinas virtuales de almacenamiento (SVM) no tiene acceso a AutoSupport.

# Añada licencias estándar basadas en controladora de SnapCenter

Una licencia estándar basada en controladora de SnapCenter es obligatoria si van a utilizar controladoras de almacenamiento FAS o AFF.

La licencia basada en controladora tiene las siguientes características:

- Autorización para licencia estándar de SnapCenter incluida con la compra de los paquetes Premium o Flash Bundle (no con el paquete básico)
- Uso de almacenamiento ilimitado
- Para habilitar esta función, se la debe añadir directamente a las controladoras de almacenamiento FAS o AFF mediante System Manager de ONTAP o la línea de comandos de clústeres de almacenamiento

  No se introduce ninguna información de licencia en la interfaz gráfica de usuario de SnapCenter para las licencias basadas en controladora de SnapCenter.

- Se bloqueó en el número de serie de la controladora

Para obtener información sobre las licencias necesarias, consulte "Licencias SnapCenter".

## Requisitos previos para añadir una licencia basada en controladora

Antes de añadir una licencia basada en controladora, debe comprobar si se instaló la licencia de Suite de SnapManager, identificar las licencias instaladas en la controladora, recuperar el número de serie de la controladora y recuperar el número de serie de la licencia basada en controladora.

### Comprobar si se ha instalado la licencia de SnapManager Suite

Puede utilizar la interfaz gráfica de usuario de SnapCenter para ver si hay una licencia de SnapManager Suite instalada en los sistemas de almacenamiento primarios FAS o AFF, e identificar qué sistemas de almacenamiento pueden requerir licencias de Suite SnapManager. Las licencias de SnapManager Suite se aplican solo a SVM de FAS y AFF o a clústeres de sistemas de almacenamiento primarios.

Si ya tiene una licencia suite de SnapManager en la controladora, la autorización para la licencia estándar basada en controladora de SnapCenter se proporciona automáticamente. Los nombres de licencia SnapManagerSuite y estándar basada en controladora de SnapCenter se utilizan indistintamente, pero se refieren a la misma licencia.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **sistemas de almacenamiento**.
  2. En la página Storage Systems, en el menú desplegable **Tipo**, seleccione si desea ver todas las SVM o clústeres que se han añadido:
     - Para ver todas las SVM que se han añadido, seleccione **ONTAP SVMs**.
     - Para ver todos los clústeres que se han agregado, seleccione **clústeres ONTAP**.

       Cuando hace clic en el nombre del clúster, todas las SVM que forman parte del clúster se muestran en la sección Storage Virtual Machines.
  3. En la lista **conexiones de almacenamiento**, busque la columna Licencia del controlador.

     La columna Controller License muestra el siguiente estado:

     - Indica que se ha instalado una licencia de SnapManager Suite en un sistema de almacenamiento primario FAS o AFF.
     - Indica que no hay una licencia de SnapManager Suite instalada en un sistema de almacenamiento primario FAS o AFF.
     - No aplicable indica que una licencia de SnapManager Suite no es aplicable debido a que la controladora de almacenamiento se encuentra en plataformas de almacenamiento Cloud Volumes ONTAP, ONTAP Select o secundario.

### Identifique las licencias instaladas en la controladora

Es posible usar la línea de comandos ONTAP para ver todas las licencias instaladas en la controladora. Debe ser un administrador de clústeres en los sistemas FAS o AFF.

En la controladora, la licencia basada en controladora SnapCenter estándar se muestra como una licencia SnapManagerSuite.

- Pasos*
  1. Inicie sesión en la controladora de NetApp mediante la línea de comandos de ONTAP.
  2. Introduzca el comando license show y a continuación, visualice el resultado para determinar si está instalada la licencia SnapManagerSuite.

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

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

Serial Number: 1-81-0000000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

En el ejemplo, la licencia SnapManagerSuite está instalada. Por lo tanto, no se requiere añadir ninguna otra licencia más con SnapCenter.

**Recupere el número de serie de la controladora**

Debe tener el número de serie de la controladora para recuperar el número de serie de su licencia basada en controladora. Para recuperar el número de serie de la controladora, utilice la línea de comandos de ONTAP. Debe ser un administrador de clústeres en los sistemas FAS o AFF.

- Pasos*
  1. Inicie sesión en la controladora con la línea de comandos de ONTAP.
  2. Introduzca el comando system show -instance y, después, revise la salida para encontrar el número de serie de la controladora.

```
cluster1::> system show -instance

Node: fas8080-41-42-01
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

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

3. Registre los números de serie.

**Recupere el número de serie de la licencia basada en controladora**

Si utiliza almacenamiento FAS o AFF, puede recuperar la licencia basada en controladora de SnapCenter desde el sitio de soporte de NetApp antes de instalarla mediante la línea de comandos de ONTAP.

**Lo que necesitará**

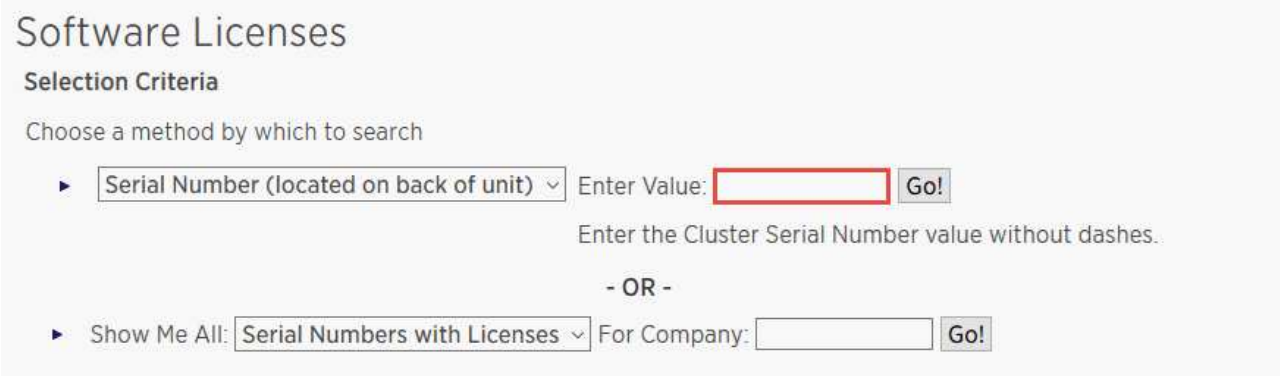
- Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.

  Si no introduce credenciales válidas, no se devuelve información a su búsqueda.

- Debe tener el número de serie de la controladora.

- Pasos*

1. Inicie sesión en el sitio de soporte de NetApp en "mysupport.netapp.com".
2. Vaya a **sistemas** > **licencias de software**.
3. En el área criterios de selección, asegúrese de que el número de serie (situado en la parte posterior de la unidad) está seleccionado, introduzca el número de serie del controlador y, a continuación, haga clic en **Ir**.




Se muestra una lista de licencias para la controladora especificada.

1. Localice y registre la licencia SnapManagerSuite o estándar de SnapCenter.

## Añada una licencia basada en controladora

Puede utilizar la línea de comandos de ONTAP para añadir una licencia basada en controladora de SnapCenter cuando utilice sistemas FAS o AFF y tenga una licencia estándar o una licencia SnapManagerSuite de SnapCenter.

### Lo que necesitará

- Debe ser un administrador de clústeres en los sistemas FAS o AFF.
- Debe tener las licencias estándar o SnapManagerSuite de SnapCenter.

### Acerca de esta tarea

Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS o AFF, puede obtener una licencia de evaluación Premium Bundle para instalarla en su controladora.

Si desea instalar SnapCenter a modo de prueba, debe ponerse en contacto con su representante de ventas para obtener una licencia de evaluación Premium Bundle para instalarla en su controladora.

- Pasos*

1. Inicie sesión en el clúster de NetApp mediante la línea de comandos ONTAP.
2. Añada la clave de licencia de SnapManagerSuite:

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

Este comando solo está disponible en el nivel de privilegios de administrador.

1. Verifique que se haya instalado la licencia de SnapManagerSuite:

```
license show
```

**Elimine la licencia de prueba**

Si utiliza una licencia estándar de SnapCenter basada en controladora y necesita eliminar la licencia de prueba basada en capacidad (número de serie que termina en «'50'»), debe utilizar comandos MySQL para eliminar manualmente la licencia de prueba. La licencia de prueba no se puede eliminar con la interfaz gráfica de usuario de SnapCenter.

> La eliminación manual de una licencia de prueba solo es necesaria si utiliza una licencia estándar basada en controladora de SnapCenter. Si adquirió una licencia basada en capacidad estándar de SnapCenter y la añade a la interfaz gráfica de usuario de SnapCenter, la licencia de prueba se sobrescribe automáticamente.

- Pasos*

1. En el servidor de SnapCenter, abra una ventana de PowerShell para restablecer la contraseña de MySQL.
   a. Ejecute el cmdlet Open-SmConnection para iniciar una sesión de conexión con SnapCenter Server para una cuenta de administrador de SnapCenter.
   b. Ejecute el comando set-SmRepositoryPassword para restablecer la contraseña de MySQL.

      Para obtener más información sobre los cmdlets de, consulte "Guía de referencia de cmdlets de SnapCenter Software".

2. Abra el símbolo del sistema y ejecute mysql -u root -p para conectarse a MySQL.

   MySQL le solicita la contraseña. Introduzca las credenciales que proporcionó al restablecer la contraseña.

3. Elimine la licencia de prueba de la base de datos:

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

# Añada licencias basadas en capacidad estándar de SnapCenter

Se utiliza una licencia de capacidad estándar de SnapCenter para proteger datos en plataformas ONTAP Select y Cloud Volumes ONTAP.

La licencia tiene las siguientes características:

- Se compone de un número de serie de nueve dígitos con el formato 51xxxxxxx

  Se utilizan el número de serie y credenciales válidas de inicio de sesión del sitio de soporte de NetApp para habilitar la licencia mediante la interfaz gráfica de usuario de SnapCenter.

- Está disponible como licencia perpetua por separado, con el coste basado en la capacidad de almacenamiento utilizada o en el tamaño de los datos que se desean proteger, el que sea más bajo, y los datos se gestionan mediante SnapCenter

- Disponible por terabytes

  Por ejemplo, puede obtener una licencia basada en capacidad para 1 TB, 2 TB, 4 TB, etc.

- Disponible como licencia de prueba de 90 días con autorización de capacidad de 100 TB

Para obtener información sobre las licencias necesarias, consulte "Licencias SnapCenter".

## Requisitos previos para añadir licencias basadas en capacidad

Antes de añadir una licencia basada en capacidad, debe calcular los requisitos de capacidad, recuperar el número de serie de la licencia basada en capacidad y, de manera opcional, generar un archivo de licencia.

### Calcular los requisitos de capacidad

Antes de obtener una licencia basada en capacidad de SnapCenter, debe calcular la cantidad de capacidad en un host que debe gestionar SnapCenter.

Debe ser un administrador de clústeres en los sistemas Cloud Volumes ONTAP o ONTAP Select.

#### Acerca de esta tarea

SnapCenter calcula la capacidad real utilizada. Si el tamaño del sistema de archivos o de la base de datos es 1 TB, pero solo se utilizan 500 GB del espacio, SnapCenter calcula los 500 GB de capacidad utilizada. La capacidad de volumen se calcula después de la deduplicación y la compresión, y se basa en la capacidad utilizada de todo el volumen.

- Pasos*

  1. Inicie sesión en la controladora de NetApp mediante la línea de comandos de ONTAP.
  2. Para ver la capacidad de volumen utilizada, escriba el comando.

     ```
     select::> vol show -fields used -volume Engineering,Marketing
     vserver volume       used
     ------- ------       ------
     VS1     Engineering  2.13TB
     VS1     Marketing    2.62TB

     2   entries were displayed.
     ```

     La capacidad utilizada combinada para los dos volúmenes es menor de 5 TB; por lo tanto, si desea proteger 5 TB de datos, el requisito mínimo de licencia basada en capacidad de SnapCenter es 5 TB.

  Sin embargo, si desea proteger solo 2 TB del total de 5 TB de capacidad utilizada total, puede adquirir una licencia basada en capacidad de 2 TB.

### Recupere el número de serie de licencia basada en capacidad

Su número de serie de licencia basada en capacidad de SnapCenter está disponible en su confirmación de pedido o en su paquete de documentación. Sin embargo, si no posee este número de serie, puede recuperarlo en el sitio de soporte de NetApp.

Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.

- Pasos*
  1. Inicie sesión en el sitio de soporte de NetApp en "mysupport.netapp.com".
  2. Vaya a **sistemas** > **licencias de software**.
  3. En el área criterios de selección, elija **SC_STANDARD** en el menú desplegable Mostrar todos: Números de serie y licencias.

  4. Escriba el nombre de su empresa y, a continuación, haga clic en **Ir**.

     Se muestra el número de serie de licencia de SnapCenter de nueve dígitos con el formato 51xxxxxxx.

  5. Registre el número de serie.

### Genere un archivo de licencia de NetApp

Si prefiere no especificar las credenciales del sitio de soporte de NetApp y el número de serie de la licencia de SnapCenter en la interfaz gráfica de usuario de SnapCenter; o si no tiene acceso a Internet al sitio de soporte de NetApp desde SnapCenter, puede generar un archivo de licencia de NetApp (NLF), A continuación, descargue y almacene el archivo en una ubicación accesible desde el host de SnapCenter.

### Lo que necesitará

- Debe usar SnapCenter con ONTAP Select o Cloud Volumes ONTAP.
- Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.
- Debe tener un número de serie de nueve dígitos de la licencia en formato 51xxxxxxx.
- Pasos*
  1. Desplácese hasta la "Generador de archivos de licencia de NetApp".
  2. Especifique la información obligatoria.
  3. En el campo línea de productos, seleccione **Estándar SnapCenter (basado en la capacidad)** en el menú desplegable.
  4. En el campo Product Serial Number, especifique el número de serie de la licencia de SnapCenter
  5. Lea y acepte la Política de privacidad de datos de NetApp y, a continuación, haga clic en **Enviar**.
  6. Guarde el archivo de licencia y, a continuación, guarde la ubicación del archivo.

## Añada una licencia basada en capacidad

Si utiliza SnapCenter con las plataformas ONTAP Select o Cloud Volumes ONTAP, debe instalar una o varias licencias basadas en capacidad de SnapCenter.

### Lo que necesitará

- Debe iniciar sesión como usuario administrador de SnapCenter.
- Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.
- Debe tener un número de serie de nueve dígitos de la licencia en formato 51xxxxxxx.

  Si desea utilizar un archivo de licencia de NetApp (NLF) para añadir la licencia, debe conocer la ubicación de ese archivo.

### Acerca de esta tarea

Puede realizar las siguientes tareas en la página Settings:

- Añadir una licencia.
- Vea los detalles de la licencia para localizar rápidamente información sobre cada licencia.
- Modifique una licencia cuando desee reemplazar la licencia existente, por ejemplo, para actualizar la capacidad de licencia o modificar la configuración de umbrales de notificación.
- Elimine una licencia cuando desee reemplazar una licencia existente o cuando ya no se necesite la licencia.

  La licencia de prueba (número de serie que finaliza con 50) no se puede eliminar mediante la interfaz gráfica de usuario de SnapCenter. La licencia de prueba se sobrescribe automáticamente cuando se añade una licencia estándar basada en capacidad de SnapCenter obtenida.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Software**.
  3. En la sección Licencia de la página Software, haga clic en **Agregar** ( + ).
  4. En el asistente Add SnapCenter License, seleccione uno de los siguientes métodos para obtener la licencia que desea añadir:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Introduzca sus credenciales de inicio de sesión en el sitio de soporte de NetApp (NSS) para importar licencias | a. Introduzca su nombre de usuario de NSS.<br>b. Introduzca su contraseña de NSS.<br>c. Introduzca el número de serie de la licencia basada en controladora. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Archivo de licencia de NetApp | a. Desplácese hasta la ubicación del archivo de licencia y selecciónelo.<br>b. Haga clic en **Abrir**. |

5. En la página Notifications, introduzca el umbral de capacidad en el que SnapCenter debe enviar notificaciones por correo electrónico, de EMS y de AutoSupport.

   El umbral predeterminado es de 90 %.

6. Para configurar el servidor SMTP para notificaciones por correo electrónico, haga clic en **Configuración** > **Configuración global** > **Configuración del servidor de notificaciones** y, a continuación, introduzca los siguientes detalles:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Preferencia de correo electrónico | Seleccione **Always** o **Never**. |
| Proporcionar configuración de correo electrónico | Si selecciona **siempre**, especifique lo siguiente:<br>• Dirección de correo electrónico del remitente<br>• Dirección de correo electrónico del destinatario<br>• Opcional: Edite la línea de asunto predeterminada<br>El asunto predeterminado es el siguiente: "Notificación de capacidad de licencia de SnapCenter". |

7. Si desea que se envíen mensajes de Event Management System (EMS) al syslog del sistema de almacenamiento o que se envíen mensajes de AutoSupport al sistema de almacenamiento debido a las operaciones con errores, seleccione las casillas de comprobación apropiadas.

   **Mejor práctica**: Se recomienda habilitar AutoSupport para ayudar a solucionar problemas que pueda experimentar.

8. Haga clic en **Siguiente**.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

### Cómo calcula SnapCenter el uso de la capacidad

SnapCenter calcula automáticamente el uso de la capacidad una vez al día a medianoche en los sistemas de almacenamiento de ONTAP Select y Cloud Volumes ONTAP que gestiona. Con el fin de garantizar una SnapCenter configurada correctamente, debe saber cómo calcula la capacidad SnapCenter.

Cuando utiliza una licencia estándar Capacity, SnapCenter calcula la capacidad sin utilizar restando la capacidad usada en todos los volúmenes de la capacidad total de la licencia. Si la capacidad utilizada supera la capacidad de la licencia, aparecerá una advertencia de uso excesivo en el panel de SnapCenter. Si ha

configurado los umbrales de capacidad y las notificaciones en SnapCenter, se enviará un correo electrónico cuando la capacidad usada llegue al umbral que haya especificado.

# Aprovisione su sistema de almacenamiento

## Aprovisionar almacenamiento en hosts Windows

### Configurar el almacenamiento de LUN

Es posible utilizar SnapCenter para configurar un LUN conectado mediante FC o mediante iSCSI. También es posible utilizar SnapCenter para conectar un LUN existente a un host Windows.

Los LUN son la unidad básica de almacenamiento en una configuración SAN. El host Windows considera a los LUN de su sistema como discos virtuales. Para obtener más información, consulte "Guía de configuración DE SAN de ONTAP 9".

#### Establecer una sesión iSCSI

Si se utiliza iSCSI para conectarse a un LUN, es necesario establecer una sesión iSCSI para poder crear el LUN y habilitar la comunicación.

**Antes de empezar**

- Definió el nodo del sistema de almacenamiento como un destino iSCSI.
- Inició el servicio iSCSI en el sistema de almacenamiento. "Leer más"

**Acerca de esta tarea**

Solo es posible establecer una sesión iSCSI entre las mismas versiones de IP, ya sea de IPv6 a IPv6 o de IPv4 a IPv4.

Es posible usar una dirección IPv6 local de vínculo para la gestión de sesiones iSCSI y la comunicación entre un host y un destino únicamente cuando ambos se encuentran en la misma subred.

El cambio de nombre de un iniciador de iSCSI afecta el acceso a los destinos iSCSI. Después de cambiar el nombre, es posible que sea necesario volver a configurar los destinos a los que accede el iniciador para que puedan reconocer el nuevo nombre. Es necesario reiniciar el host después de cambiar el nombre de un iniciador de iSCSI.

Si el host tiene más de una interfaz de iSCSI, una vez que se establece una sesión iSCSI con SnapCenter mediante una dirección IP en la primera interfaz, no se puede establecer una sesión iSCSI desde otra interfaz con una dirección IP diferente.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **iSCSI Session**.
  3. En la lista desplegable **Storage Virtual Machine**, seleccione la máquina virtual de almacenamiento (SVM) para el destino iSCSI.
  4. En la lista desplegable **Host**, seleccione el host para la sesión.

5. Haga clic en **establecer sesión**.

   Se mostrará el asistente Establish Session.

6. En el asistente Establish Session, identifique el destino:

| En este campo… | Introduzca… |
|---|---|
| Nombre del nodo de destino | El nombre de nodo del destino iSCSI<br><br>Si ya existe un nombre de nodo de destino, el nombre se muestra en formato de solo lectura. |
| Dirección del portal de destino | La dirección IP del portal de red de destino |
| Puerto del portal de destino | El puerto TCP del portal de red de destino |
| Dirección del portal del iniciador | La dirección IP del portal de red del iniciador |

7. Cuando esté satisfecho con las entradas, haga clic en **conectar**.

   SnapCenter establecerá la sesión iSCSI.

8. Repita este procedimiento para establecer una sesión para cada destino.

#### Desconecte una sesión iSCSI

En algunas ocasiones, es posible que sea necesario desconectar una sesión iSCSI de un destino en el que existen varias sesiones.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **iSCSI Session**.
  3. En la lista desplegable **Storage Virtual Machine**, seleccione la máquina virtual de almacenamiento (SVM) para el destino iSCSI.
  4. En la lista desplegable **Host**, seleccione el host para la sesión.
  5. En la lista de sesiones iSCSI, seleccione la sesión que desea desconectar y haga clic en **desconectar sesión**.
  6. En el cuadro de diálogo desconectar sesión, haga clic en **Aceptar**.

     SnapCenter desconectará la sesión iSCSI.

#### Cree y gestione grupos

Es posible crear grupos de iniciadores (iGroup) para especificar los hosts que pueden acceder a un LUN determinado en el sistema de almacenamiento. Se puede usar SnapCenter para crear un igroup en un host de Windows, cambiar su nombre, modificarlo o eliminarlo.

### Cree un igroup

Es posible usar SnapCenter para crear un igroup en un host de Windows. El igroup se mostrará en el asistente Create Disk o Connect Disk al asignar el igroup a un LUN.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **iGroup**.
  3. En la página iGroups, haga clic en **Nuevo**.
  4. En el cuadro de diálogo Create iGroup, defina el igroup:

| En este campo… | Realice lo siguiente… |
|---|---|
| Sistema de almacenamiento | Seleccione la máquina virtual de almacenamiento SVM para el LUN que desea asignar al igroup. |
| Host | Seleccione el host en el que desea crear el igroup. |
| Nombre del iGroup | Introduzca el nombre del igroup. |
| Iniciadores | Seleccione el iniciador. |
| Tipo | Seleccione el tipo de iniciador, iSCSI, FCP o mixto (FCP e iSCSI). |

  5. Cuando se sienta conforme con las entradas, haga clic en **Aceptar**.

     SnapCenter creará el igroup en el sistema de almacenamiento.

### Cambiar el nombre de un igroup

Es posible utilizar SnapCenter para cambiar el nombre de un igroup existente.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **iGroup**.
  3. En la página Initiator Groups, haga clic en el campo **Storage Virtual Machine** para mostrar una lista de las SVM disponibles y, a continuación, seleccione la SVM para el igroup cuyo nombre desea cambiar.
  4. En la lista de iGroup de la SVM, seleccione el igroup cuyo nombre desea cambiar y haga clic en **Rename**.
  5. En el cuadro de diálogo Rename igroup, introduzca el nuevo nombre para el igroup y haga clic en **Rename**.

### Modificar un igroup

Es posible usar SnapCenter para añadir iniciadores de igroups a un grupo existente. Durante la creación de un igroup, puede añadir un solo host. Si desea crear un igroup para un clúster, puede modificar el igroup a fin de añadir nodos a ese igroup.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **iGroup**.
  3. En la página Initiator Groups, haga clic en el campo **Storage Virtual Machine** para mostrar una lista desplegable de SVM disponibles y seleccione la SVM para el igroup que desea modificar.
  4. En la lista de grupos de iniciadores, seleccione un igroup y haga clic en **Add Initiator to igroup**.
  5. Seleccione un host.
  6. Seleccione los iniciadores y haga clic en **Aceptar**.

### Eliminar un igroup

Es posible usar SnapCenter para eliminar un igroup cuando ya no se necesita.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **iGroup**.
  3. En la página Initiator Groups, haga clic en el campo **Storage Virtual Machine** para mostrar una lista desplegable de las SVM disponibles y seleccione la SVM para el igroup que desea eliminar.
  4. En la lista de grupos de iniciadores de la SVM, seleccione el igroup que desea eliminar y haga clic en **Delete**.
  5. En el cuadro de diálogo Delete igroup, haga clic en **OK**.

     SnapCenter eliminará el igroup.

#### Crear y gestionar discos

El host de Windows ve los LUN en el sistema de almacenamiento como discos virtuales. Es posible usar SnapCenter para crear y configurar un LUN conectado a FC o conectado a iSCSI.

SnapCenter no admite cambiar el nombre de un disco. Si se cambia el nombre de un disco gestionado por SnapCenter, se producirá un error en las operaciones de SnapCenter.

### Ver los discos en un host

Es posible ver los discos en cada host Windows que administra con SnapCenter.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.

3. Seleccione el host en la lista desplegable **Host**.

   Se muestra una lista de los discos.

### Vea los discos en clúster

Puede ver los discos en clúster en el clúster que gestiona con SnapCenter. Los discos en clúster solo se muestran cuando selecciona el clúster en el menú desplegable hosts.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.
  3. Seleccione el clúster en la lista desplegable **Host**.

     Se muestra una lista de los discos.

### Crear LUN o discos conectados mediante FC o iSCSI

El host de Windows ve los LUN en el sistema de almacenamiento como discos virtuales. Es posible usar SnapCenter para crear y configurar un LUN conectado a FC o conectado a iSCSI.

#### Lo que necesitará

- Creó un volumen para el LUN en su sistema de almacenamiento.

  El volumen solo debe contener LUN y solo LUN creados con SnapCenter.

  > No se puede crear un LUN en un volumen de clones creado en SnapCenter a menos que el clon ya se encuentre dividido.

- Inició el servicio iSCSI o FC en el sistema de almacenamiento.
- Si utiliza iSCSI, debe haber establecido una sesión iSCSI con el sistema de almacenamiento.
- El paquete de plugins de SnapCenter para Windows debe instalarse únicamente en el host donde se crea el disco.

#### Acerca de esta tarea

- No se puede conectar un LUN a más de un host a menos que el LUN se comparta entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.
- Si un LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server donde se utilizan volúmenes compartidos de clúster (CSV), es necesario crear el disco en el host propietario del grupo de clústeres.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.
  3. Seleccione el host en la lista desplegable **Host**.
  4. Haga clic en **Nuevo**.

Se abrirá el asistente Create Disk.

5. En la página LUN Name, identifique el LUN:

| En este campo… | Realice lo siguiente… |
|---|---|
| Sistema de almacenamiento | Seleccione la máquina virtual de almacenamiento SVM para el LUN. |
| Ruta de LUN | Haga clic en **examinar** para seleccionar la ruta completa de la carpeta que contiene el LUN. |
| Nombre de LUN | Introduzca el nombre del LUN. |
| Tamaño del clúster | Seleccione el tamaño de la asignación de bloques LUN para el clúster.<br><br>El tamaño del clúster varía según el sistema operativo y las aplicaciones. |
| Etiqueta de LUN | De forma opcional, puede introducir un texto descriptivo para el LUN. |

6. En la página Disk Type, seleccione el tipo de disco:

| Seleccione… | Si… |
|---|---|
| Disco dedicado | Solo un host puede acceder al LUN.<br><br>Ignore el campo **Grupo de recursos**. |
| Disco compartido | El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.<br><br>Introduzca el nombre del grupo de recursos del clúster en el campo **Grupo de recursos**. Es necesario crear el disco en un solo host del clúster de conmutación al nodo de respaldo. |
| Volumen compartido de clúster (CSV) | El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server donde se utilizan volúmenes compartidos de clúster.<br><br>Introduzca el nombre del grupo de recursos del clúster en el campo **Grupo de recursos**. Asegúrese de que el host en el que se crea el disco sea el propietario del grupo de clústeres. |

7. En la página Drive Properties, especifique las propiedades de la unidad:

| Propiedad | Descripción |
| --- | --- |
| Asignación automática del punto de montaje | SnapCenter asigna de forma automática un punto de montaje de volumen según la unidad del sistema.<br><br>Por ejemplo, si la unidad del sistema es C:, la asignación automática crea un punto de montaje de volumen debajo de la unidad C: (C:\scmnpt\). La asignación automática no es compatible con los discos compartidos. |
| Asignar letra de unidad | Monte el disco en la unidad seleccionada en la lista desplegable adyacente. |
| Utilice punto de montaje de volumen | Monte el disco en la ruta de unidad especificada en el campo adyacente.<br><br>La raíz del punto de montaje de volumen debe ser propiedad del host en el que se crea el disco. |
| No asigne la letra de unidad ni el punto de montaje de volumen | Seleccione esta opción si prefiere montar el disco manualmente en Windows. |
| Tamaño de LUN | Especifique el tamaño del LUN; el valor mínimo es 150 MB.<br><br>Seleccione MB, GB o TB en la lista desplegable contigua. |
| Use thin provisioning para el volumen que aloja este LUN | Aprovisione con thin provisioning el LUN.<br><br>Thin provisioning solo asigna la cantidad de espacio de almacenamiento que se necesita en un momento. Esto permite que el LUN se expanda de forma eficiente hasta la capacidad máxima disponible.<br><br>Asegúrese de que el espacio disponible en el volumen sea suficiente para acomodar todo el almacenamiento de LUN que considere necesario. |

| Propiedad | Descripción |
| --- | --- |
| Elija el tipo de partición | Seleccione una partición GPT para una tabla de particiones GUID o una partición MBR para un registro de arranque maestro.<br><br>Las particiones MBR pueden generar problemas de desalineación en los clústeres de conmutación al nodo de respaldo de Windows Server.<br><br>No se admiten los discos de partición de firmware extensible unificado (UEFI). |

8. En la página Map LUN, seleccione el iniciador de iSCSI o FC en el host:

| En este campo… | Realice lo siguiente… |
| --- | --- |
| Host | Haga doble clic en el nombre del grupo de clústeres para ver una lista desplegable de los hosts que pertenecen al clúster y, a continuación, seleccione el host para el iniciador.<br><br>Este campo solo se muestra si el LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server. |
| Elija iniciador del host | Seleccione **Fibre Channel** o **iSCSI** y, a continuación, seleccione el iniciador en el host.<br><br>Puede seleccionar varios iniciadores de FC si utiliza FC con I/o multivía (MPIO). |

9. En la página Group Type, especifique si desea asignar un igroup existente al LUN o crear un igroup nuevo:

| Seleccione… | Si… |
| --- | --- |
| Cree un nuevo igroup para los iniciadores seleccionados | Desea crear un nuevo igroup para los iniciadores seleccionados. |
| Seleccione un igroup existente o especifique un nuevo igroup para los iniciadores seleccionados | Desea especificar un igroup existente para los iniciadores seleccionados o crear un nuevo igroup con el nombre que especifique.<br><br>Escriba el nombre del igroup en el campo **igroup name**. Escriba las primeras letras del nombre del igroup existente para que el campo se complete automáticamente. |

10. En la página Resumen, revise las selecciones y, a continuación, haga clic en **Finalizar**.

    SnapCenter creará el LUN y lo conectará a la unidad o la ruta de unidad especificadas en el host.

### Cambiar el tamaño de un disco

Es posible aumentar o reducir el tamaño de un disco a medida que el sistema de almacenamiento necesite cambiar.

**Acerca de esta tarea**

- Para las LUN con thin provisioning, el tamaño de la geometría de las lun de ONTAP se muestra como el tamaño máximo.
- Para el LUN con aprovisionamiento grueso, se muestra el tamaño expandible (tamaño disponible en el volumen) como tamaño máximo.
- Los LUN con particiones tipo MBR tienen un límite de tamaño de 2 TB.
- Los LUN con particiones tipo GPT tienen un límite de tamaño del sistema de almacenamiento de 16 TB.
- Se recomienda realizar una copia de Snapshot antes de cambiar el tamaño de un LUN.
- Si se necesita restaurar un LUN de una copia de Snapshot realizada antes de cambiar el tamaño del LUN, SnapCenter cambia automáticamente el tamaño del LUN al tamaño de la copia de Snapshot.

  Después de la operación de restauración, los datos añadidos a la LUN después de cambiar su tamaño deben restaurarse a partir de una copia Snapshot realizada después de cambiar su tamaño.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.
  3. Seleccione el host en la lista desplegable Host.

     Se muestra una lista de los discos.

  4. Seleccione el disco cuyo tamaño desea cambiar y, a continuación, haga clic en **Cambiar tamaño**.
  5. En el cuadro de diálogo Resize Disk, use la herramienta deslizante para especificar el tamaño nuevo del disco, o bien introduzca el tamaño nuevo en el campo Size.

     Si introduce el tamaño manualmente, debe hacer clic fuera del campo Size para que los botones Shrink o Expand se habiliten según sea apropiado. Además, debe hacer clic en MB, GB o TB para especificar la unidad de medida.

  6. Cuando se sienta conforme con las entradas, haga clic en **Shrink** o **Expand**, según corresponda.

     SnapCenter cambiará el tamaño del disco.

### Conectar un disco

Es posible usar el asistente Connect Disk para conectar un LUN existente a un host o volver a conectar un LUN que se ha desconectado.

**Lo que necesitará**

- Inició el servicio iSCSI o FC en el sistema de almacenamiento.
- Si utiliza iSCSI, debe haber establecido una sesión iSCSI con el sistema de almacenamiento.
- No se puede conectar un LUN a más de un host a menos que el LUN se comparta entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.
- Si el LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server donde se utilizan volúmenes compartidos de clúster (CSV), es necesario conectar el disco en el host propietario del grupo de clústeres.
- Se debe instalar el plugin para Windows únicamente en el host donde se conecta el disco.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. En la página hosts, haga clic en **Disks**.
3. Seleccione el host en la lista desplegable **Host**.
4. Haga clic en **conectar**.

   Se abrirá el asistente Connect Disk.

5. En la página LUN Name, identifique el LUN al que se desea conectar:

| En este campo… | Realice lo siguiente… |
|---|---|
| Sistema de almacenamiento | Seleccione la máquina virtual de almacenamiento SVM para el LUN. |
| Ruta de LUN | Haga clic en **examinar** para seleccionar la ruta completa del volumen que contiene el LUN. |
| Nombre de LUN | Introduzca el nombre del LUN. |
| Tamaño del clúster | Seleccione el tamaño de la asignación de bloques LUN para el clúster.<br><br>El tamaño del clúster varía según el sistema operativo y las aplicaciones. |
| Etiqueta de LUN | De forma opcional, puede introducir un texto descriptivo para el LUN. |

6. En la página Disk Type, seleccione el tipo de disco:

| Seleccione… | Si… |
|---|---|
| Disco dedicado | Solo un host puede acceder al LUN. |

| Seleccione… | Si… |
| --- | --- |
| Disco compartido | El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.<br><br>Solo es necesario conectar el disco a un host del clúster de conmutación al nodo de respaldo. |
| Volumen compartido de clúster (CSV) | El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server donde se utilizan volúmenes compartidos de clúster.<br><br>Asegúrese de que el host en el que se conecta al disco sea el propietario del grupo de clústeres. |

7. En la página Drive Properties, especifique las propiedades de la unidad:

| Propiedad | Descripción |
| --- | --- |
| Asignación automática | Permita que SnapCenter asigne de forma automática un punto de montaje de volumen según la unidad del sistema.<br><br>Por ejemplo, si la unidad del sistema es C:, la propiedad de asignación automática crea un punto de montaje de volumen debajo de la unidad C: (C:\scmnpt\). La propiedad de asignación automática no es compatible con los discos compartidos. |
| Asignar letra de unidad | Monte el disco en la unidad seleccionada en la lista desplegable contigua. |
| Utilice punto de montaje de volumen | Monte el disco en la ruta de unidad especificada en el campo contiguo.<br><br>La raíz del punto de montaje de volumen debe ser propiedad del host en el que se crea el disco. |
| No asigne la letra de unidad ni el punto de montaje de volumen | Seleccione esta opción si prefiere montar el disco manualmente en Windows. |

8. En la página Map LUN, seleccione el iniciador de iSCSI o FC en el host:

| En este campo… | Realice lo siguiente… |
| --- | --- |
| Host | Haga doble clic en el nombre del grupo de clústeres para ver una lista desplegable de los hosts que pertenecen al clúster y, a continuación, seleccione el host para el iniciador.<br><br>Este campo solo se muestra si el LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server. |
| Elija iniciador del host | Seleccione **Fibre Channel** o **iSCSI** y, a continuación, seleccione el iniciador en el host.<br><br>Puede seleccionar varios iniciadores de FC si utiliza FC con MPIO. |

9. En la página Group Type, especifique si desea asignar un igroup existente al LUN o crear un igroup nuevo:

| Seleccione… | Si… |
| --- | --- |
| Cree un nuevo igroup para los iniciadores seleccionados | Desea crear un nuevo igroup para los iniciadores seleccionados. |
| Seleccione un igroup existente o especifique un nuevo igroup para los iniciadores seleccionados | Desea especificar un igroup existente para los iniciadores seleccionados o crear un nuevo igroup con el nombre que especifique.<br><br>Escriba el nombre del igroup en el campo **igroup name**. Escriba las primeras letras del nombre del igroup existente para que el campo se complete automáticamente. |

10. En la página Resumen, revise las selecciones y haga clic en **Finalizar**.

    SnapCenter conecta el LUN a la unidad o la ruta de unidad especificada en el host.

### Desconectar un disco

Es posible desconectar un LUN de un host sin afectar el contenido del LUN, con una excepción: Si se desconecta un clon antes de haberlo dividido, se pierde el contenido del clon.

**Lo que necesitará**

- Asegúrese de que ninguna aplicación utilice el LUN.
- Asegúrese de que el LUN no se supervise con software de supervisión.
- Si el LUN es compartido, asegúrese de quitar las dependencias de recursos de clúster del LUN y verificar que todos los nodos en el clúster estén encendidos, funcionen correctamente y estén disponibles para SnapCenter.

**Acerca de esta tarea**

Si desconecta un LUN en un volumen FlexClone que ha creado SnapCenter y ningún otro LUN del volumen está conectado, SnapCenter lo elimina. Antes de desconectar el LUN, SnapCenter muestra un mensaje para advertir que se puede eliminar el volumen de FlexClone.

Para evitar la eliminación automática del volumen de FlexClone, se recomienda cambiar el nombre del volumen antes de desconectar el último LUN. Al cambiar el nombre del volumen, asegúrese de cambiar varios caracteres, no solo el último carácter del nombre.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.
  3. Seleccione el host en la lista desplegable **Host**.

     Se muestra una lista de los discos.
  4. Seleccione el disco que desea desconectar y haga clic en **desconectar**.
  5. En el cuadro de diálogo desconectar disco, haga clic en **Aceptar**.

     SnapCenter desconectará el disco.

**Eliminar un disco**

Es posible eliminar un disco cuando ya no se necesita. Después de eliminar un disco, no se puede recuperar.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.
  3. Seleccione el host en la lista desplegable **Host**.

     Se muestra una lista de los discos.
  4. Seleccione el disco que desea eliminar y, a continuación, haga clic en **Eliminar**.
  5. En el cuadro de diálogo Eliminar disco, haga clic en **Aceptar**.

     SnapCenter eliminará el disco.

**Cree y gestione recursos compartidos de SMB**

Para configurar un recurso compartido de SMB3 en una máquina virtual de almacenamiento (SVM), se puede usar la interfaz de usuario de SnapCenter o cmdlets de PowerShell.

**Mejor práctica:** se recomienda utilizar los cmdlets porque le permite aprovechar las plantillas proporcionadas con SnapCenter para automatizar la configuración de recursos compartidos.

Las plantillas engloban prácticas recomendadas para configuraciones de volúmenes y recursos compartidos. Las plantillas se encuentran en la carpeta Templates de la carpeta de instalación para el paquete de plugins

de SnapCenter para Windows.

Si se siente cómodo, puede seguir los modelos proporcionados para crear sus propias plantillas. Debe revisar los parámetros en la documentación de cmdlet antes de crear una plantilla personalizada.

#### Cree un recurso compartido de SMB

Puede usar la página SnapCenter Shares para crear un recurso compartido de SMB3 en una máquina virtual de almacenamiento (SVM).

No se puede usar SnapCenter para realizar backups de bases de datos en recursos compartidos de SMB. La compatibilidad con SMB se limita al aprovisionamiento.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **shares**.
  3. Seleccione la SVM de la lista desplegable **Storage Virtual Machine**.
  4. Haga clic en **Nuevo**.

     Se abrirá el cuadro de diálogo New Share.

  5. En el cuadro de diálogo New Share, defina el recurso compartido:

| En este campo… | Realice lo siguiente… |
|---|---|
| Descripción | Introduzca un texto descriptivo para el recurso compartido. |
| Nombre del recurso compartido | Introduzca el nombre del recurso compartido, por ejemplo, test_share.<br><br>El nombre que se introduce para el recurso compartido también se utiliza como nombre del volumen.<br><br>El nombre del recurso compartido:<br><br>• Debe ser una cadena UTF-8.<br>• No debe incluir los siguientes caracteres: Caracteres de control de 0x00 a 0x1F (ambos inclusive), 0x22 (comillas dobles) y los caracteres especiales `\ / [ ] : (vertical bar) < > + = ; , ?` |

| En este campo… | Realice lo siguiente… |
| --- | --- |
| Comparta la ruta | • Haga clic en el campo para introducir una nueva ruta de acceso al sistema de archivos, por ejemplo, /.<br>• Haga doble clic en el campo para seleccionar una de la lista de rutas de acceso al sistema de archivos. |

6. Cuando se sienta conforme con las entradas, haga clic en **Aceptar**.

   SnapCenter creará el recurso compartido de SMB en la SVM.

#### Eliminar un recurso compartido de SMB

Es posible eliminar un recurso compartido de SMB cuando ya no se necesita.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **shares**.
  3. En la página Shares, haga clic en el campo **Storage Virtual Machine** para ver una lista desplegable de las máquinas virtuales de almacenamiento (SVM) disponibles y seleccione la SVM para el recurso compartido que desea eliminar.
  4. En la lista de recursos compartidos de la SVM, seleccione el recurso que desea eliminar y haga clic en **Eliminar**.
  5. En el cuadro de diálogo Eliminar recurso compartido, haga clic en **Aceptar**.

     SnapCenter eliminará el recurso compartido de SMB de la SVM.

### Recupere espacio en el sistema de almacenamiento

Si bien NTFS hace un seguimiento del espacio disponible en un LUN cuando se modifican o se eliminan archivos, no provee la nueva información al sistema de almacenamiento. Es posible ejecutar la recuperación de espacio mediante el cmdlet de PowerShell en el host del plugin para Windows a fin de garantizar que los bloques recién liberados se marquen como disponibles en el almacenamiento.

Si ejecuta el cmdlet en un host de plugin remoto, debe ejecutar el cmdlet SnapCenterOpen-SMConnection para abrir una conexión con el servidor de SnapCenter.

#### Lo que necesitará

- Antes de ejecutar una operación de restauración, debe asegurarse de que el proceso de recuperación de espacio se haya completado.
- Si el LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server, debe ejecutar la recuperación de espacio en el host propietario del grupo de clústeres.
- Para que el almacenamiento alcance un rendimiento óptimo, la recuperación de espacio debe ejecutarse con la mayor frecuencia posible.

Debe asegurarse de que se haya analizado el sistema de archivos NTFS completo.

**Acerca de esta tarea**

- La recuperación de espacio consume mucho tiempo y recursos de CPU, por lo que generalmente se recomienda ejecutar la operación cuando el uso del sistema de almacenamiento y del host de Windows es bajo.
- En la recuperación de espacio, se recupera casi todo el espacio disponible, aunque no el 100 %.
- No debe ejecutar la desfragmentación del disco al mismo tiempo que está realizando la recuperación de espacio.

  Ya que al hacerlo se ralentiza el proceso de recuperación.

**Paso**

Desde el símbolo del sistema de PowerShell en el servidor de aplicaciones, escriba el siguiente comando:

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

Drive_path es la ruta de la unidad asignada al LUN.

#### Aprovisionar el almacenamiento mediante cmdlets de PowerShell

Si no desea utilizar la interfaz gráfica de usuario de SnapCenter para realizar trabajos de aprovisionamiento de hosts y reclamación de espacio, puede utilizar los cmdlets de PowerShell que ofrece el plugin de SnapCenter para Microsoft Windows. Puede usar los cmdlets directamente o añadirlos a scripts.

Si ejecuta los cmdlets en el host de un plugin remoto, debe ejecutar el cmdlet SnapCenter Open-SMConnection para abrir una conexión con el servidor SnapCenter.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Aprovisione almacenamiento en entornos VMware

Es posible usar el plugin de SnapCenter para Microsoft Windows en entornos de VMware para crear y gestionar LUN, así como para gestionar las copias de Snapshot.

#### Plataformas de sistemas operativos invitados compatibles con VMware

- Versiones compatibles de Windows Server
- Configuraciones de clústeres de Microsoft

  Compatible con un máximo de 16 nodos admitidos en VMware al usar el iniciador de software iSCSI de Microsoft, o hasta dos nodos usando FC

- LUN de RDM

  Compatible con un máximo de 56 LUN de RDM con cuatro controladoras SCSI LSI Logic para RDMS

normales, o 42 LUN de RDM con tres controladoras SCSI LSI Logic en una configuración del plugin para Windows de buzón a buzón MSCS para máquinas virtuales VMware

Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

#### Limitaciones relacionadas con el servidor ESXi de VMware

- No se admite la instalación del plugin para Windows en un clúster de Microsoft de máquinas virtuales donde se utilizan credenciales de ESXi.

  Al instalar el plugin para Windows en máquinas virtuales almacenadas en clúster, se deben utilizar credenciales de vCenter.

- Todos los nodos almacenados en clúster deben utilizar el mismo ID objetivo (en el adaptador SCSI virtual) para el mismo disco almacenado en clúster.
- Cuando se crea un LUN de RDM fuera del plugin para Windows, es necesario reiniciar el servicio de plugin para que este pueda reconocer el disco recientemente creado.
- No se pueden utilizar iniciadores de iSCSI y FC al mismo tiempo en un sistema operativo invitado de VMware.

#### Privilegios mínimos de vCenter requeridos para operaciones de RDM en SnapCenter

Debe tener los siguientes privilegios de vCenter en el host para ejecutar operaciones de RDM en un sistema operativo invitado:

- Almacén de datos: Quitar archivo
- Host: Configuración > Configuración de la partición de almacenamiento
- Máquina virtual: Configuración

Debe asignar estos privilegios a una función en el nivel de Virtual Center Server. El rol al que se asignen estos privilegios no puede asignarse a quien no tenga privilegios de usuario raíz.

Después de asignar estos privilegios, puede instalar el plugin para Windows en el sistema operativo invitado.

### Gestione LUN de RDM FC en un clúster de Microsoft

Es posible utilizar el plugin para Windows para gestionar un clúster de Microsoft mediante LUN de RDM FC, pero primero es necesario crear el quórum de RDM compartido y el almacenamiento compartido fuera del plugin, para luego añadir los discos a las máquinas virtuales del clúster.

A partir de ESXi 5.5, también es posible utilizar hardware ESX iSCSI y FCoE para gestionar un clúster de Microsoft. El plugin para Windows incluye soporte preconfigurado para clústeres de Microsoft.

#### Requisitos

El plugin para Windows ofrece compatibilidad con clústeres de Microsoft que utilizan LUN de RDM FC en dos máquinas virtuales distintas que pertenecen a dos servidores ESX o ESXi diferentes, también denominadas clústeres en todos los cuadros, cuando se satisfacen requisitos de configuración específicos.

- Las máquinas virtuales (VM) deben ejecutar la misma versión de Windows Server.
- Las versiones del servidor ESX o ESXi deben ser las mismas para cada host primario de VMware.

- Cada host primario debe tener al menos dos adaptadores de red.
- Debe haber al menos un almacén de datos de VMware Virtual Machine File System (VMFS) compartido entre los dos servidores ESX o ESXi.
- VMware recomienda que el almacén de datos compartido se cree en una FC SAN.

  Si es necesario, el almacén de datos compartido también puede crearse a través de iSCSI.

- El LUN de RDM compartido debe estar en modo de compatibilidad física.
- El LUN de RDM compartido debe crearse manualmente fuera del plugin para Windows.

  No se pueden usar discos virtuales para almacenamiento compartido.

- Debe haber una controladora SCSI configurada en cada máquina virtual en el clúster que se encuentra en modo de compatibilidad física:

  Windows Server 2008 R2 requiere que configure la controladora SCSI LSI Logic SAS en cada máquina virtual. Los LUN compartidos no pueden utilizar las controladoras LSI Logic SAS si solo existe una de su tipo y ya está conectada a la unidad C.

  No se admiten controladoras SCSI de tipo paravirtual en clústeres de Microsoft de VMware.

  Cuando agrega un controlador SCSI a un LUN compartido en una máquina virtual en modo de compatibilidad física, debe seleccionar la opción **asignaciones de dispositivos sin formato** (RDM) y no la opción **Crear un nuevo disco** en VMware Infrastructure Client.

- Los clústeres de máquinas virtuales de Microsoft no pueden formar parte de un clúster de VMware.
- Es necesario utilizar credenciales de vCenter, no de ESX o ESXi al instalar el plugin para Windows en máquinas virtuales que pertenecen a un clúster de Microsoft.
- El plugin para Windows no puede crear un iGroup individual con iniciadores de varios hosts.

  El igroup que contiene los iniciadores de todos los hosts ESXi debe crearse en la controladora de almacenamiento antes de crear los LUN de RDM que se utilizarán como discos de clústeres compartidos.

- Asegúrese de crear un LUN de RDM en ESXi 5.0 con un iniciador FC.

  Cuando se crea un LUN de RDM, se crea un iGroup con ALUA.

#### Limitaciones

El plugin para Windows admite clústeres de Microsoft cuando se utilizan LUN de RDM FC/iSCSI en máquinas virtuales diferentes pertenecientes a servidores ESX o ESXi diferentes.

Esta función no es compatible con las versiones anteriores a ESX 5.5i.

- El plugin para Windows no admite clústeres en almacenes de datos ESX iSCSI y NFS.
- El plugin para Windows no admite iniciadores mixtos en un entorno de clústeres.

  Los iniciadores deben ser FC o Microsoft iSCSI, pero no ambos.

- No se admiten los iniciadores de ESX iSCSI y los adaptadores de bus de host en los discos compartidos de un clúster de Microsoft.

- El plugin para Windows no admite la migración de máquinas virtuales con vMotion si las máquinas virtuales forman parte de un clúster de Microsoft.
- El plugin para Windows no admite MPIO en máquinas virtuales de un clúster de Microsoft.

#### Cree un LUN de RDM FC compartido

Para poder utilizar LUN de RDM FC a fin de compartir almacenamiento entre los nodos de un clúster de Microsoft, primero es necesario crear el disco de quórum compartido y el disco de almacenamiento compartido, y añadirlos a las dos máquinas virtuales en el clúster.

El disco compartido no se crea mediante el plugin para Windows. Debe crear y luego agregar el LUN compartido a cada máquina virtual del clúster. Para obtener más información, consulte "Equipos virtuales en clúster entre hosts físicos".

# Configure las conexiones MySQL protegidas con SnapCenter Server

Es posible generar certificados de capa de sockets seguros (SSL) y archivos de claves para proteger la comunicación entre SnapCenter Server y MySQL Server en configuraciones independientes o configuraciones de balanceo de carga de red (NLB).

## Configure conexiones MySQL protegidas para configuraciones de servidor SnapCenter independientes

Es posible generar certificados de capa de sockets seguros (SSL) y archivos de claves para proteger la comunicación entre SnapCenter Server y MySQL Server. Los certificados y los archivos de claves se deben configurar en MySQL Server y SnapCenter Server.

Se generan los siguientes certificados:

- Certificado de CA
- Archivo de claves privadas y certificado público de servidor
- Archivo de claves privadas y certificado público de cliente
- Pasos*

1. Para configurar los certificados de SSL y los archivos de claves para servidores y clientes MySQL en Windows, utilice el comando openssl.

   Para obtener más información, consulte "MySQL versión 5.7: Creación de claves y certificados SSL mediante openssl"

   > El valor de nombre común que se usa para el certificado de servidor, el certificado de cliente y los archivos de claves debe ser distinto del valor de nombre común que se utiliza para el certificado de CA. Si los valores de nombre común son los mismos, el certificado y los archivos de claves producen errores en los servidores compilados con OpenSSL.

   **Mejor práctica:** debe utilizar el nombre de dominio completo (FQDN) del servidor como nombre común para el certificado de servidor.

2. Copie los certificados de SSL y los archivos de claves en la carpeta MySQL Data.

   La ruta predeterminada de la carpeta MySQL Data es `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Actualice las rutas del certificado de CA, del certificado público de servidor, del certificado público de cliente, de la clave privada de servidor y de la clave privada de cliente en el archivo de configuración del servidor MySQL (my.ini).

   La ruta predeterminada del archivo de configuración del servidor MySQL (my.ini) es `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > Debe especificar las rutas del certificado de CA, del certificado público de servidor y de la clave privada de servidor en la sección [mysqld] del archivo de configuración del servidor MySQL (my.ini).

   Debe especificar las rutas del certificado de CA, del certificado público de cliente y de la clave privada de cliente en la sección [client] del archivo de configuración del servidor MySQL (my.ini).

   En el siguiente ejemplo, se muestran los certificados y los archivos de claves copiados en la sección [mysqld] del archivo my.ini en la carpeta predeterminada `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   En el siguiente ejemplo, se muestran las rutas actualizadas en la sección [client] del archivo my.inil.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
   ```

4. Detenga la aplicación web del servidor SnapCenter en el servidor de información de Internet (IIS).

5. Reinicie el servicio MySQL.
6. Actualice el valor de la clave MySQLProtocol en el archivo web.config.

   En el siguiente ejemplo, se muestra el valor de la clave MySQLProtocol actualizada en el archivo web.config.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Actualice el archivo web.config con las rutas proporcionadas en la sección [client] del archivo my.inil.

   En el siguiente ejemplo, se muestran las rutas actualizadas en la sección [client] del archivo my.inil.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

+

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

+

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

1. Inicie la aplicación web del servidor SnapCenter en IIS.

## Configure conexiones MySQL protegidas para configuraciones de alta disponibilidad

Es posible generar certificados de capa de sockets seguros (SSL) y archivos de claves para los dos nodos de alta disponibilidad (ha) a fin de proteger la comunicación entre SnapCenter Server y los servidores MySQL. Los certificados y los archivos de claves se deben configurar en las instancias de MySQL Server y en los nodos ha.

Se generan los siguientes certificados:

- Certificado de CA

  Se genera un certificado de CA en uno de los nodos ha, y este certificado de CA se copia en el otro nodo ha.

- Certificado público de servidor y archivos de claves privadas de servidor en los dos nodos de alta disponibilidad
- Certificado público de cliente y archivos de claves privadas de cliente en los dos nodos de alta disponibilidad

- Pasos*

1. Para el primer nodo ha, configure los certificados de SSL y los archivos de claves para servidores y clientes MySQL en Windows con el comando openssl.

   Para obtener más información, consulte "MySQL versión 5.7: Creación de claves y certificados SSL mediante openssl"

   > El valor de nombre común que se usa para el certificado de servidor, el certificado de cliente y los archivos de claves debe ser distinto del valor de nombre común que se utiliza para el certificado de CA. Si los valores de nombre común son los mismos, el certificado y los archivos de claves producen errores en los servidores compilados con OpenSSL.

   **Mejor práctica:** debe utilizar el nombre de dominio completo (FQDN) del servidor como nombre común para el certificado de servidor.

2. Copie los certificados de SSL y los archivos de claves en la carpeta MySQL Data.

   La ruta predeterminada de la carpeta MySQL Data es C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Actualice las rutas del certificado de CA, del certificado público de servidor, del certificado público de cliente, de la clave privada de servidor y de la clave privada de cliente en el archivo de configuración del servidor MySQL (my.ini).

   La ruta predeterminada del archivo de configuración del servidor MySQL (my.ini) es C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.inI.

   > Debe especificar las rutas del certificado de CA, del certificado público de servidor y de la clave privada de servidor en la sección [mysqld] del archivo de configuración del servidor MySQL (my.ini).

   Debe especificar las rutas del certificado de CA, del certificado público de cliente y de la clave privada de cliente en la sección [client] el archivo de configuración del servidor MySQL (my.ini).

   En el siguiente ejemplo, se muestran los certificados y los archivos de claves copiados en la sección [mysqld] del archivo my.ini en la carpeta predeterminada C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

En el siguiente ejemplo, se muestran las rutas actualizadas en la sección [client] del archivo my.inil.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. Para el segundo nodo ha, copie el certificado de CA y genere un certificado público de servidor, archivos de claves privadas de servidor, un certificado público de cliente y archivos de claves privadas de cliente. siga estos pasos:

   a. En la carpeta MySQL Data del segundo nodo NLB, copie el certificado de CA generado en el primer nodo de alta disponibilidad.

      La ruta predeterminada de la carpeta MySQL Data es C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

      > No debe volver a crear un certificado de CA. Debe crear únicamente el certificado público de servidor, el certificado público de cliente, el archivo de claves privadas de servidor y el archivo de claves privadas de cliente.

   b. Para el primer nodo ha, configure los certificados de SSL y los archivos de claves para servidores y clientes MySQL en Windows con el comando openssl.

      "MySQL versión 5.7: Creación de claves y certificados SSL mediante openssl"

      > El valor de nombre común que se usa para el certificado de servidor, el certificado de cliente y los archivos de claves debe ser distinto del valor de nombre común que se utiliza para el certificado de CA. Si los valores de nombre común son los mismos, el certificado y los archivos de claves producen errores en los servidores compilados con OpenSSL.

      Se recomienda usar el nombre de dominio completo del servidor como nombre común para el certificado del servidor.

   c. Copie los certificados de SSL y los archivos de claves en la carpeta MySQL Data.

   d. Actualice las rutas del certificado de CA, del certificado público de servidor, del certificado público de cliente, de la clave privada de servidor y de la clave privada de cliente en el archivo de configuración del servidor MySQL (my.ini).

      > Debe especificar las rutas del certificado de CA, del certificado público de servidor y de la clave privada de servidor en la sección [mysqld] del archivo de configuración del servidor MySQL (my.ini).

Debe especificar las rutas del certificado de CA, del certificado público de cliente y de la clave privada de cliente en la sección [client] del archivo de configuración del servidor MySQL (my.ini).

En el siguiente ejemplo, se muestran los certificados y los archivos de claves copiados en la sección [mysqld] del archivo my.ini en la carpeta predeterminada C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

En el siguiente ejemplo, se muestran las rutas actualizadas en la sección [client] del archivo my.inil.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. Detenga la aplicación web del servidor SnapCenter en el servidor de información de Internet (IIS) en los dos nodos ha.
6. Reinicie el servicio MySQL en los dos nodos ha.
7. Actualice el valor de la clave MySQLProtocol del archivo web.config en los dos nodos de alta disponibilidad.

   En el siguiente ejemplo, se muestra el valor de la clave MySQLProtocol actualizada en el archivo web.config.

```
<add key="MySQLProtocol" value="SSL" />
```

8. Actualice el archivo web.config con las rutas especificadas en la sección [client] del archivo my.ini en los dos nodos de alta disponibilidad.

   En el siguiente ejemplo, se muestran las rutas actualizadas en la sección [client] de los archivos my.inil.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

+

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

+

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

1. Inicie la aplicación web servidor SnapCenter en IIS en los dos nodos ha.
2. Use el cmdlet Set-SmRepositoryConfig -RebuildSlave -Force de PowerShell con la opción -Force en uno de los nodos de alta disponibilidad para establecer la replicación de MySQL protegida en los dos nodos de alta disponibilidad.

   Aunque el estado de la replicación sea correcto, la opción -Force permite reconstruir el repositorio esclavo.

# Funciones habilitadas en su host de Windows durante la instalación

El instalador de SnapCenter Server habilita las funciones de Windows y los roles en el host de Windows durante la instalación Esto puede ser interesante en el caso de que tenga que realizar labores de solución de problemas y de mantenimiento en el sistema del host.

| Categoría | Función |
| --- | --- |
| Servidor web | • Servicios de Información de Internet<br>• Servicio World Wide Web<br>• Características HTTP comunes<br>◦ Documento predeterminado<br>◦ Exploración de directorios<br>◦ Errores HTTP<br>◦ Redirección HTTP<br>◦ Contenido estático<br>◦ Publicación en WebDAV<br>• Estado y diagnóstico<br>◦ Registro personalizado<br>◦ Registro HTTP<br>◦ Herramientas de registro<br>◦ Supervisor de solicitudes<br>◦ Seguimiento<br>• Características de rendimiento<br>◦ Compresión de contenido estático<br>• Seguridad<br>◦ Seguridad IP<br>◦ Autenticación básica<br>◦ Compatibilidad centralizada con certificados SSL<br>◦ Autenticación por asignación de certificados de clientes<br>◦ Autenticación de asignaciones de certificado de cliente de IIS<br>◦ Restricciones de IP y dominio<br>◦ Filtrado de solicitudes<br>◦ Autorización para URL<br>◦ Autenticación de Windows<br>• Características de desarrollo de aplicaciones<br>◦ Extensibilidad de .NET 4.5<br>◦ Inicialización de aplicaciones<br>◦ ASP.NET 4.5<br>◦ Inclusión del lado servidor<br>◦ Protocolo WebSocket<br>• Herramientas de gestión<br>Consola de gestión de IIS |

| Categoría | Función |
| --- | --- |
| Scripts y herramientas de gestión de IIS | • Servicio de gestión de IIS<br>• Herramientas de gestión web |
| .NET Framework 4.5.2 Características | • .NET Framework 4.5.2<br>• ASP.NET 4.5.2<br>• Activación HTTP de Windows Communication Foundation (WCF) 45<br>◦ Activación de TCP<br>◦ Activación HTTP<br>◦ Activación de Message Queuing (MSMQ) |
| Cola de mensajes | • Servicios de Message Queue Server<br>Asegúrese de que ninguna otra aplicación utiliza el servicio MSMQ que SnapCenter crea y administra.<br>• Servidor MSMQ |
| Servicio de activación de procesos de Windows | • Modelo de proceso |
| API de configuración | Todo |

# Proteger bases de datos de Microsoft SQL Server

## Plugin de SnapCenter para Microsoft SQL Server

### Información general sobre el plugin de SnapCenter para Microsoft SQL Server

El plugin de SnapCenter para Microsoft SQL Server es un componente en el lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de bases de datos de Microsoft SQL Server. El plugin para SQL Server automatiza las operaciones de backup, verificación, restauración y clonado de bases de datos de SQL Server en el entorno de SnapCenter.

Cuando se instala el plugin para SQL Server, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear copias de reflejo de conjuntos de backups en otro volumen, y también con la tecnología SnapVault de NetApp para realizar replicaciones de backup disco a disco para cumplimiento de normativas o fines de archivado.

### Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft SQL Server

Cuando el plugin de SnapCenter para Microsoft SQL Server está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar bases de datos de SQL Server.

Es posible ejecutar las siguientes tareas complementarias a las operaciones de backup, de restauración y de clonado de las bases de datos de SQL Server y sus recursos:

- Realizar backup de bases de datos de SQL Server y los registros de transacciones asociados

  No es posible crear un backup de registros para las bases de datos maestra y msdb. Sin embargo, puede crear backups de registros para la base de datos modelo del sistema.

- Restaurar recursos de bases de datos
  - Se pueden restaurar bases de datos de sistema maestras, msdb y modelo.
  - No es posible restaurar varias bases de datos, instancias y grupos de disponibilidad.
  - No puede restaurar la base de datos del sistema en una ruta alternativa.
- Crear clones de un momento específico para las bases de datos de producción

  No es posible ejecutar operaciones de backup, restauración, clonado o ciclo de vida en las bases de datos del sistema tempdb.

- Verifique las operaciones de backup de inmediato o aplace la verificación hasta más adelante

  No se admite la verificación de la base de datos del sistema SQL Server. SnapCenter clona las bases de datos para realizar una operación de verificación. SnapCenter no puede clonar bases de datos del sistema SQL Server y, por lo tanto, no se admite la verificación de estas bases de datos.

- Programar operaciones de backup y de clonado
- Supervisar operaciones de backup, de restauración y de clonado

El plugin para SQL Server no es compatible con el backup y la recuperación de las bases de datos de SQL Server en los recursos compartidos SMB.

## Funciones del plugin de SnapCenter para Microsoft SQL Server

El plugin para SQL Server se integra con Microsoft SQL Server en el host Windows y con la tecnología de copia de Snapshot de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para SQL Server, se utiliza la interfaz de SnapCenter.

El plugin para SQL Server incluye estas características principales:

- **Interfaz gráfica de usuario unificada con tecnología SnapCenter**

  La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar procesos de backup y restauración consistentes entre plugins, utilizar informes centralizados, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins. SnapCenter además ofrece gestión de políticas y programación centralizada para admitir operaciones de backup y clonado.

- **Administración central automatizada**

  Es posible programar backups rutinarios de SQL Server, configurar retención de backups basada en políticas y configurar operaciones de restauración de momento específico y de último minuto. Si desea supervisar de manera proactiva el entorno de SQL Server, configure SnapCenter para que envíe alertas por correo electrónico.

- **Tecnología de copia snapshot de NetApp** no disruptiva

  El plugin para SQL Server utiliza la tecnología de copia de Snapshot de NetApp con el plugin de SnapCenter para Microsoft Windows de NetApp. Esto permite realizar backups de bases de datos en cuestión de segundos y restaurarlos rápidamente sin necesidad de dejar sin conexión a SQL Server. Las copias de Snapshot consumen un espacio de almacenamiento mínimo.

Además de estas funciones principales, el plugin para SQL Server ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración, clonado y verificación
- Seguridad compatible con RBAC y delegación de roles centralizada
- Creación de copias de bases de datos de producción con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

  Se requiere una licencia de FlexClone en el sistema de almacenamiento donde está el clon.

- Verificación de backups no disruptiva y automatizada
- Capacidad para ejecutar varios backups al mismo tiempo entre varios servidores
- Cmdlets de PowerShell para crear scripts de operaciones de backup, verificación, restauración y clonado
- Compatibilidad con grupos de disponibilidad (AG) AlwaysOn en SQL Server para acelerar las operaciones de configuración, backup y restauración de AG

- Base de datos en memoria y extensión de espacio libre (BPE) como parte de SQL Server 2014
- Compatibilidad con backup de LUN y VMDK
- Compatibilidad con infraestructuras físicas y virtualizadas
- Compatibilidad con iSCSI, Fibre Channel, FCoE, asignación de dispositivos sin formato (RDM) y VMDK sobre NFS y VMFS

  Los volúmenes NAS deben tener una política de exportación predeterminada en la máquina virtual de almacenamiento (SVM).

- Compatibilidad con FileStream y grupos de archivos en bases de datos independientes de SQL Server.

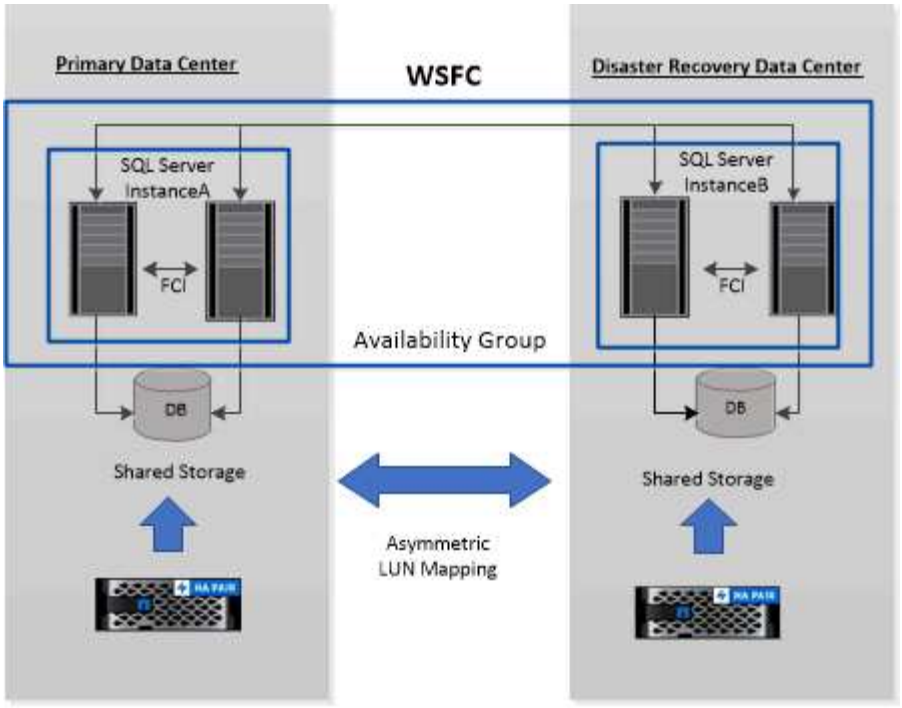
## Compatibilidad con asignación de LUN asimétrica en clústeres de Windows

El plugin de SnapCenter para Microsoft SQL Server admite la detección en SQL Server 2012 y posterior, configuraciones de asignación de LUN asimétrica (ALM) para alta disponibilidad y grupos de disponibilidad para recuperación ante desastres. Al detectar recursos, SnapCenter detecta bases de datos en host locales y remotos en configuraciones de ALM.

Una configuración de ALM es un solo clúster de conmutación al nodo de respaldo del servidor Windows que contiene uno o varios nodos en un centro de datos primario y uno o varios nodos en un centro de recuperación ante desastres.

A continuación se muestra un ejemplo de configuración de ALM:

- Dos instancias de clúster de conmutación al nodo de respaldo (FCI) en un centro de datos multisitio
- FCI for local High Availability (ha) y Availability Group (AG) para la recuperación ante desastres con una instancia independiente en el centro de recuperación ante desastres




WSFC----Windows Server Failover Cluster

El almacenamiento en el centro de datos principal se comparte entre los nodos FCI presentes en el centro de datos principal. El almacenamiento en el centro de datos de recuperación ante desastres se comparte entre los nodos FCI presentes en el centro de datos de recuperación ante desastres.

El almacenamiento del centro de datos principal no es visible para los nodos en el centro de datos de recuperación ante desastres y viceversa.

La arquitectura DE ALM combina dos soluciones de almacenamiento compartido utilizadas por FCI con una solución de almacenamiento no compartido o dedicado utilizada por SQL AG. La solución AG utiliza letras de unidad idénticas para los recursos de discos compartidos entre centros de datos. Esta disposición de almacenamiento, donde un disco de clúster se comparte entre un subconjunto de nodos dentro de un WSFC, se conoce como ALM.

## Tipos de almacenamiento compatibles con los plugins de SnapCenter para Microsoft Windows y Microsoft SQL Server

SnapCenter es compatible con una gran variedad de tipos de almacenamiento, tanto en máquinas físicas como virtuales. Antes de instalar el paquete para el host, es necesario verificar que el tipo de almacenamiento sea compatible.

Windows Server es compatible con el aprovisionamiento y la protección de datos de SnapCenter. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
|---|---|---|---|
| Servidor físico | LUN conectados a FC | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
| --- | --- | --- | --- |
| Servidor físico | LUN conectados a iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Servidor físico | Recursos compartidos de SMB3 (CIFS) que residen en una máquina virtual de almacenamiento (SVM) | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Compatibilidad solo para aprovisionamiento.<br><br>No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB. |
| Máquina virtual de VMware | LUN de RDM conectados por un adaptador de bus de host FC o iSCSI | Cmdlets de PowerShell | |
| Máquina virtual de VMware | LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Máquina virtual de VMware | Sistemas de archivos de máquina virtual (VMFS) o almacenes de datos NFS | VSphere de VMware | |
| Máquina virtual de VMware | Un sistema invitado conectado a recursos compartidos de SMB3 que residen en una SVM | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Compatibilidad solo para aprovisionamiento.<br><br>No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB. |

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
| --- | --- | --- | --- |
| Máquina virtual Hyper-V. | LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Para aprovisionar LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual se debe usar Hyper-V Manager.<br>No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |
| Máquina virtual Hyper-V. | LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
|---|---|---|---|
| Máquina virtual Hyper-V. | Un sistema invitado conectado a recursos compartidos de SMB3 que residen en una SVM | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Compatibilidad solo para aprovisionamiento.<br><br>No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB.<br><br>No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |

## Recomendaciones sobre distribución de almacenamiento para el plugin de SnapCenter para Microsoft SQL Server

Una buena distribución de almacenamiento permite que SnapCenter Server realice backups de bases de datos para que pueda cumplir sus objetivos de recuperación. Se deben tener en cuenta diferentes factores al definir la distribución de almacenamiento, como el tamaño de la base de datos, la tasa de cambio de la base de datos y la frecuencia con la que se realizan backups.

Las siguientes secciones definen las recomendaciones y restricciones de distribución de almacenamiento para LUN y discos de máquina virtual (VMDK) con el plugin de SnapCenter para Microsoft SQL Server instalado en el entorno.

En este caso, los LUN pueden incluir discos VMware RDM y LUN iSCSI de conexión directa asignados al invitado de the guest.

### Requisitos de LUN y VMDK

Opcionalmente, puede utilizar LUN o VMDK específicos para optimizar el rendimiento y la gestión de las siguientes bases de datos:

- Bases de datos maestra y de sistema modelo
- Tempdb

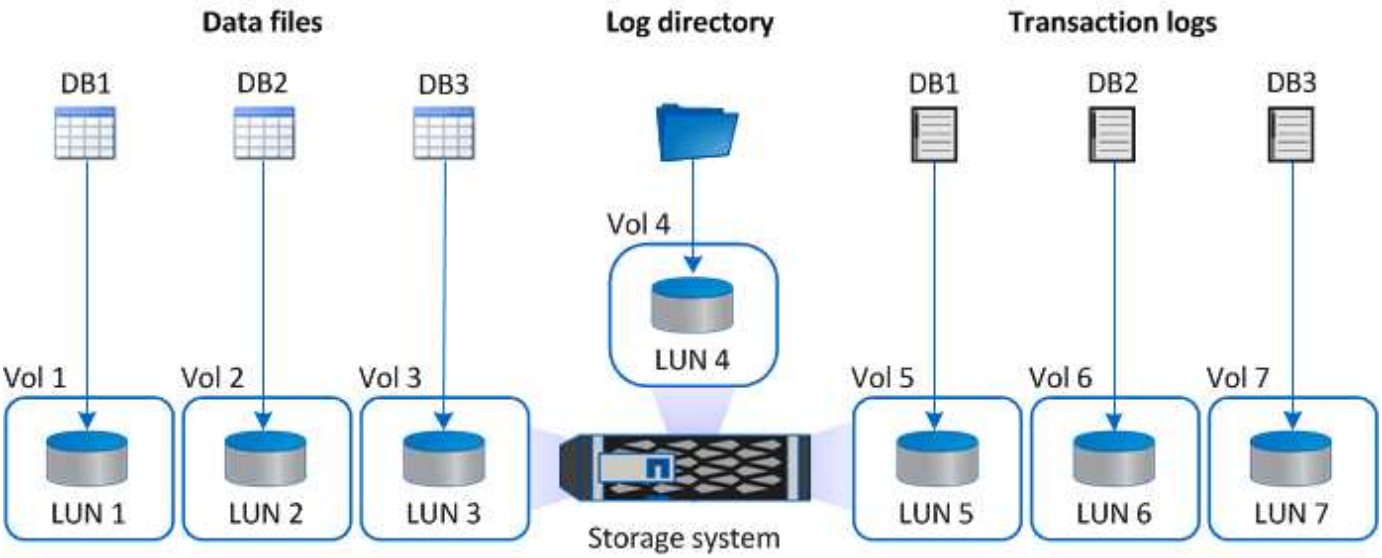
- Archivos de bases de datos del usuario (.mdf y .ndf)
- Archivos de registro de transacciones de bases de datos (.ldf)
- Directorio de registro

Para restaurar grandes bases de datos, la práctica recomendada es utilizar LUN o VMDK específicos El tiempo que se necesita para restaurar un LUN o un VMDK completos es inferior al que se requiere para restaurar los archivos individuales almacenados en el LUN o el VMDK

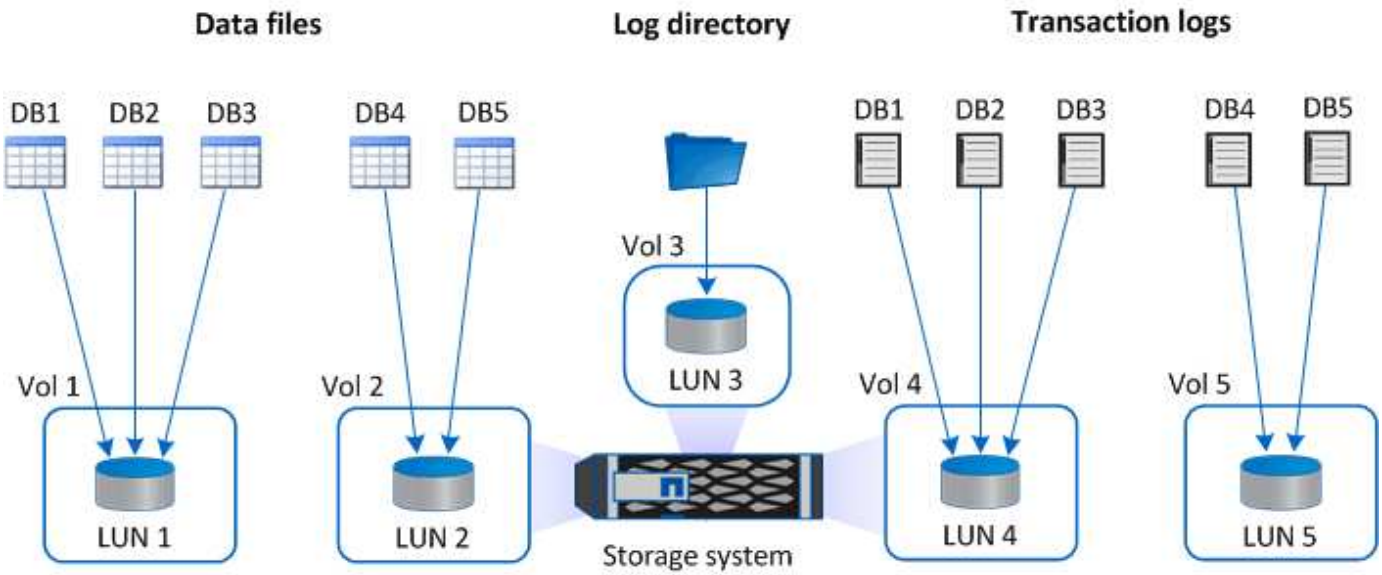
Para el directorio de registro, deber crear un LUN o un VMDK por separado para que haya espacio libre suficiente en los discos de archivos de registro o archivos de datos

### Ejemplos de distribución de LUN y VMDK

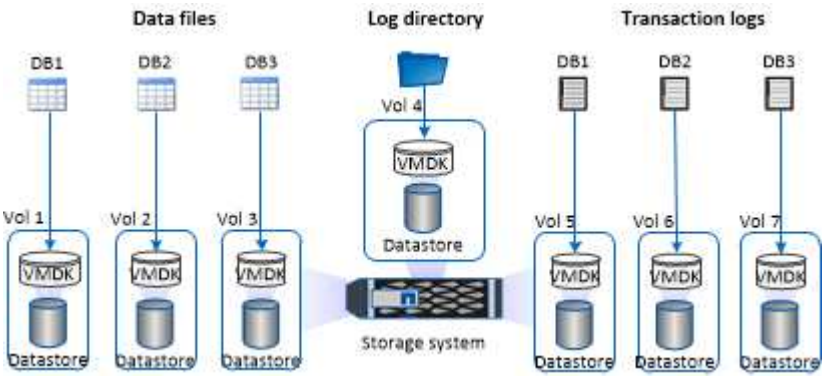
El gráfico siguiente muestra cómo puede configurar la distribución almacenamiento para bases de datos grandes en LUN:



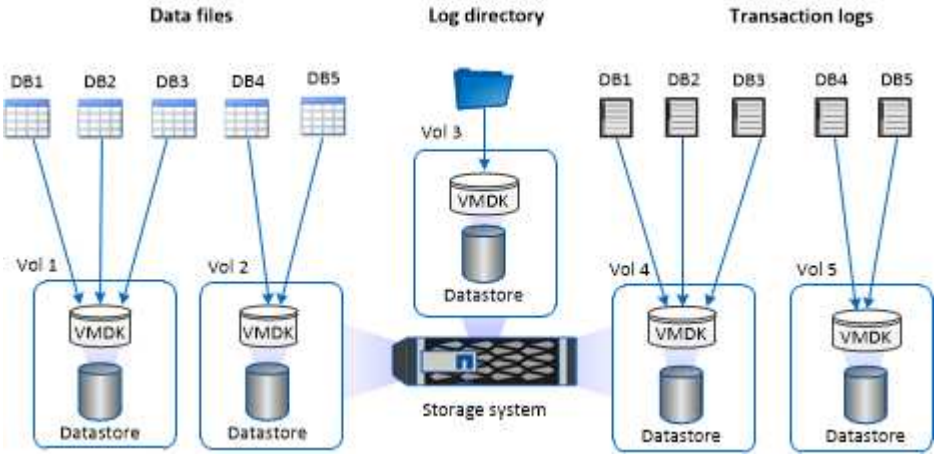

El gráfico siguiente muestra cómo puede configurar la distribución de almacenamiento para bases de datos medianas o pequeñas en LUN:



El gráfico siguiente muestra cómo puede configurar la distribución almacenamiento para bases de datos grandes en VMDK:




El gráfico siguiente muestra cómo puede configurar la distribución de almacenamiento para bases de datos medianas o pequeñas en VMDK:




## Privilegios mínimos de ONTAP requeridos para el plugin de SQL

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

| **Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores** |
| --- |
| event generate-autosupport-log |
| se muestra el historial del trabajo<br>detención de trabajo |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| lun |
| lun create |
| eliminación de lun |
| igroup de lun añadido |
| crear lun igroup |
| lun igroup eliminado |
| cambio de nombre de lun igroup |
| lun igroup show |
| asignación de lun de nodos adicionales |
| se crea la asignación de lun |
| se elimina la asignación de lun |
| asignación de lun quitar nodos de generación de informes |
| se muestra el mapa de lun |
| modificación de lun |
| movimiento de lun en volumen |
| lun desconectada |
| lun conectada |
| cambio de tamaño de lun |
| serie de lun |
| muestra de lun |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| regla adicional de la política de snapmirror<br>regla de modificación de la política de snapmirror<br>regla de eliminación de la política de snapmirror<br>la política de snapmirror<br>restauración de snapmirror<br>de snapmirror<br>historial de snapmirror<br>actualización de snapmirror<br>conjunto de actualizaciones de snapmirror<br>destinos de listas de snapmirror |
| versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| crear el clon de volumen |
| show de clon de volumen |
| inicio de división de clon de volumen |
| detención de división de clon de volumen |
| cree el volumen |
| destrucción del volumen |
| crear el archivo de volumen |
| uso show-disk del archivo de volumen |
| volumen sin conexión |
| volumen en línea |
| modificación del volumen |
| crear el qtree de volúmenes |
| eliminación de qtree de volumen |
| modificación del qtree del volumen |
| se muestra volume qtree |
| restricción de volumen |
| visualización de volumen |
| crear snapshots de volumen |
| eliminación de snapshots de volumen |
| modificación de las copias de snapshot de volumen |
| cambio de nombre de copias de snapshot de volumen |
| restauración de copias snapshot de volumen |
| archivo de restauración de snapshots de volumen |
| visualización de copias de snapshot de volumen |
| desmonte el volumen |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| vserver cifs |
| vserver cifs share create |
| eliminación de vserver cifs share |
| se muestra vserver shadowcopy |
| visualización de vserver cifs share |
| visualización de vserver cifs |
| política de exportación de vserver |
| creación de política de exportación de vserver |
| eliminación de la política de exportación de vserver |
| creación de reglas de política de exportación de vserver |
| aparece la regla de política de exportación de vserver |
| visualización de la política de exportación de vserver |
| vserver iscsi |
| se muestra la conexión iscsi del vserver |
| se muestra vserver |

| Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| interfaz de red |
| se muestra la interfaz de red |
| vserver |
| MetroCluster show |

## Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para SQL Server

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

## Estrategia de backup para recursos de SQL Server

### Defina una estrategia de backup para recursos de SQL Server

Definir una estrategia de backup antes de crear las tareas de backup ayuda a garantizar que se cuente con todos los backups necesarios para restaurar o clonar correctamente las bases de datos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el objetivo de punto de recuperación contribuyen a la estrategia de backup.

### Tipo de backups admitido

El backup de bases de datos SQL Server del sistema y del usuario con SnapCenter requiere seleccionar el tipo de recurso, como bases de datos, instancias de SQL Server y grupos de disponibilidad (AG). Se aprovecha la tecnología de copia de Snapshot para crear copias en línea y de solo lectura de los volúmenes donde residen los recursos.

Puede seleccionar la opción de solo copia para especificar que SQL Server no trunque los registros de transacciones. Debe utilizar esta opción cuando gestiona SQL Server con otras aplicaciones de backup. Mantener intactos los registros de transacciones permite que cualquier aplicación de backup restaure las bases de datos del sistema. Los backups de solo copia son independientes de la secuencia de backups programados, y no afectan los procedimientos de backup y restauración de la base de datos.

| Tipo de backup | Descripción | Opción de solo copia con el tipo de backup |
| --- | --- | --- |
| Backup completo y backup de registros | Realiza un backup de la base de datos del sistema y acorta los registros de transacciones.<br><br>La instancia de SQL Server acorta los registros de transacciones eliminando las entradas que ya están confirmadas en la base de datos.<br><br>Después de finalizar el backup completo, esta opción crea un registro de transacciones que captura la información de la transacción. En términos generales, debe elegir esta opción. Sin embargo, si el tiempo de backup es corto, puede optar por no ejecutar un backup del registro de transacciones junto con el backup completo.<br><br>No es posible crear un backup de registros para las bases de datos maestra y msdb. Sin embargo, puede crear backups de registros para la base de datos modelo del sistema. | Realiza un backup de los archivos de la base de datos del sistema y los registros de transacciones sin acortarlos.<br><br>Un backup de solo copia actúa como un backup de la base diferencial o un backup diferencial, y no afecta la base diferencial. Restaurar un backup completo de solo copia es igual que restaurar cualquier otro backup completo. |
| Backup completo de la base de datos | Realiza un backup de los archivos de la base de datos del sistema.<br><br>Es posible crear un backup completo de la base de datos para las bases de datos maestra, modelo y msdb del sistema. | Realiza un backup de los archivos de la base de datos del sistema. |
| Backup de registros de transacciones | Realiza un backup de los registros de transacciones acortados, copiando solo las transacciones que se confirmaron desde el backup más reciente del registro de transacciones.<br><br>Si programa backups del registro de transacciones frecuentes junto con backups completos de la base de datos, puede elegir puntos de recuperación granulares. | Realiza un backup de los registros de transacciones sin acortarlos.<br><br>Este tipo de backup no afecta la secuencia de los backups de registros regulares. Los backups de registros solo de copia son útiles para realizar operaciones de restauración en línea |

### Programaciones de backups para el plugin para SQL Server

La frecuencia de los backups (tipo de programación) se especifica en las políticas; la programación de los backups se especifica en la configuración del grupo de recursos. El factor más crítico para determinar la frecuencia o la programación de los backups es la tasa de cambio del recurso y la importancia de los datos. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores son la importancia del recurso para la organización, el SLA y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso en el caso de un recurso utilizado intensivamente, no existe el requisito de ejecutar un backup completo más de una o dos veces al día. Por ejemplo, es posible que sea suficiente realizar backups regulares de registros de transacciones para garantizar los backups necesarios Cuanto mayor sea la frecuencia con que realiza backups de las bases de datos, menos registros de transacciones deberá utilizar SnapCenter en el momento de la restauración, lo que puede dar como resultado operaciones más rápidas.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de los backups (cada cuánto tiempo deben realizarse los backups), denominada *schedule type* para algunos plugins, forma parte de la configuración de una política. Se puede seleccionar una frecuencia de backups por hora, por día, por semana o por mes para la política. Si no selecciona ninguna de estas frecuencias, la política creada es de sólo bajo demanda. Puede acceder a las directivas haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

  Las programaciones de los backups (el momento exacto en que se realizan los backups) forman parte de una configuración de grupo de recursos. Por ejemplo, si tiene un grupo de recursos que posee una política configurada para backups semanales, quizás sea conveniente configurar la programación para que realice backups todos los jueves a las 00:10. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **grupos de recursos**.

### Cantidad de tareas de backup necesarias para bases de datos

Algunos factores que determinan la cantidad de tareas de backup que se necesitan son el tamaño de la base de datos, la cantidad de volúmenes que se usan, la tasa de cambio de la base de datos y el acuerdo de nivel de servicio.

Para los backups de bases de datos, la cantidad de trabajos de backup que se selecciona depende de la cantidad de volúmenes en los que se colocaron las bases de datos. Por ejemplo, si se colocó un grupo de bases de datos pequeñas en un volumen y una base de datos grande en otro volumen, puede ser necesario crear un trabajo de backup para las bases de datos pequeñas y otro trabajo para la base de datos grande.

### Convenciones de nomenclatura de backups para el plugin para SQL Server

Es posible usar la convención de nomenclatura de copia Snapshot predeterminada o usar una convención de nomenclatura personalizada. La convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de las copias de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La copia Snapshot usa la siguiente convención de nomenclatura predeterminada:

```
resourcegroupname_hostname_timestamp
```

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre de host.
- *03-12-2015_23.17.26* es la fecha y la marca de hora.

Como alternativa, puede especificar el formato de nombre de la copia Snapshot mientras protege los recursos o grupos de recursos seleccionando **usar formato de nombre personalizado para copia Snapshot**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la copia de Snapshot.

#### Opciones de retención de backups para el plugin para SQL Server

Es posible elegir la cantidad de días durante los cuales se retendrán las copias de backup o especificar la cantidad de copias de backup que se desean retener, con un máximo de 255 copias en ONTAP. Por ejemplo, una organización puede necesitar retener 10 días de copias de backup o 130 copias de backup.

Al crear una política, es posible especificar las opciones de retención para cada tipo y programación de backup.

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

SnapCenter elimina los backups previos que tengan etiquetas de retención que coincidan con el tipo de programación. Si se modifica el tipo de programación para el recurso o el grupo de recursos, los backups con la etiqueta del tipo de programación anterior podrían conservarse en el sistema.

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

#### Cuánto tiempo se retienen los backups de registros de transacciones en el sistema de almacenamiento de origen

El plugin de SnapCenter para Microsoft SQL Server necesita backups de registros de transacciones para ejecutar operaciones de restauración de último minuto, que restauran la base de datos a un momento entre dos backups completos.

Por ejemplo, si el plugin para SQL Server hizo un backup completo a las 8:00 y otro backup completo a las 8:00 p. m., se podía utilizar el último backup de registros de transacciones para restaurar la base de datos a cualquier momento entre las 5:00 y las 5:00 Si no se cuenta con registros de transacciones, el plugin para SQL Server solamente puede ejecutar operaciones de restauración a un momento específico, que restaura una base de datos al momento en que el plugin para SQL Server finalizó un backup completo.

En general, se requieren operaciones de restauración de último minuto únicamente durante un día o dos. De forma predeterminada, SnapCenter conserva un mínimo de dos días.

#### Varias bases de datos en el mismo volumen

Es posible colocar todas las bases de datos en el mismo volumen, ya que la política de backup incluye una opción para configurar la cantidad máxima de bases de datos por backup (el valor predeterminado es 100).

Por ejemplo, si hay 200 bases de datos en el mismo volumen, se crean dos copias de Snapshot con 100 bases de datos en cada copia.

#### Verificación de copias de backup con un volumen de almacenamiento primario o secundario para el plugin para SQL Server

Es posible verificar las copias de backups en el volumen de almacenamiento principal o en el volumen de almacenamiento secundario de SnapMirror y SnapVault. La verificación con un volumen de almacenamiento secundario reduce la carga para el volumen de almacenamiento principal.

Cuando se verifica un backup que se encuentra en el volumen de almacenamiento primario o secundario, todas las copias de Snapshot primarias y secundarias se marcan como verificadas.

Se necesita una licencia de SnapRestore para verificar copias de backup en un volumen de almacenamiento secundario de SnapMirror o SnapVault.

#### Cuándo programar tareas de verificación

Si bien SnapCenter puede verificar los backups de inmediato después de crearlos, esta tarea puede aumentar significativamente el tiempo necesario para finalizar la tarea de backup y consume muchos recursos. Por lo tanto, casi siempre es conveniente programar la verificación en una tarea independiente más tarde. Por ejemplo, si se realiza el backup de una base de datos a las 5:00 todos los días, se puede programar la verificación una hora después, a las 6:00

Por el mismo motivo, generalmente no es necesario ejecutar una verificación de backup cada vez que se realiza un backup. Ejecutar la verificación regularmente aunque con un intervalo menos frecuente suele ser suficiente para garantizar la integridad del backup. Una misma tarea de verificación puede verificar varios backups a la vez.

## Estrategia de restauración para SQL Server

#### Defina una estrategia de restauración para SQL Server

Definir una estrategia de restauración para SQL Server permite restaurar correctamente la base de datos.

#### Orígenes y destinos para una operación de restauración

Es posible restaurar una base de datos de SQL Server desde una copia de backup en el almacenamiento primario o secundario. También es posible restaurar la base de datos a diferentes destinos además de su ubicación original, para poder elegir el destino que

cumpla determinados requisitos.

#### Orígenes para una operación de restauración

Es posible restaurar bases de datos desde almacenamiento primario o secundario.

#### Destinos para una operación de restauración

Es posible restaurar bases de datos a varios destinos:

| Destino | Descripción |
|---|---|
| La ubicación original | De forma predeterminada, SnapCenter restaura la base de datos a la misma ubicación y en la misma instancia de SQL Server. |
| Otra ubicación | Es posible restaurar la base de datos a otra ubicación en cualquier instancia de SQL Server dentro del mismo host. |
| Ubicación original u otra ubicación con otro nombre de la base de datos | Es posible restaurar la base de datos con otro nombre a cualquier instancia de SQL Server en el mismo host donde se creó el backup. |

No se admite la restauración en un host alternativo entre servidores ESX para bases de datos de SQL en VMDK (NFS y almacenes de datos de VMFS).

### Modelos de recuperación de SQL Server admitidos por SnapCenter

De forma predeterminada, se asignan modelos de recuperación específicos a cada tipo de base de datos. El administrador de la base de datos de SQL Server puede reasignar cada base de datos a otro modelo de recuperación.

SnapCenter admite tres tipos de modelos de recuperación de SQL Server:

- Modelo de recuperación simple

  Cuando utiliza el modelo de recuperación simple, no puede realizar un backup de los registros de transacciones.

- Modelo de recuperación completa

  Cuando se utiliza el modelo de recuperación completa, es posible restaurar una base de datos a su estado anterior desde el punto de error.

- Modelo de recuperación de registro masivo

  Cuando se utiliza el modelo de recuperación de registro masivo, debe volver a ejecutarse manualmente la operación de registro masivo. Debe realizar la operación de registro masivo si antes de la restauración no se ha realizado un backup del registro de transacciones que contiene el registro de confirmación de la operación. Si la operación de registro masivo inserta 10 millones de filas en una base de datos, y la base de datos genera errores antes de someterse a un backup, la base de datos restaurada no incluye las filas

que se insertaron en la operación de registro masivo.

### Tipos de operaciones de restauración

Es posible usar SnapCenter para ejecutar diferentes tipos de operaciones de restauración de los recursos de SQL Server.

- Restauración de último minuto
- Restauración a un momento específico

Es posible hacer una restauración de último minuto o a un momento específico previo en las siguientes situaciones:

- Restauración desde un almacenamiento secundario de SnapMirror o SnapVault
- Restauración en una ruta (ubicación) alternativa

SnapCenter no es compatible con SnapRestore basado en volúmenes.

#### Restauración de último minuto

En una operación de restauración de último minuto (seleccionada de forma predeterminada), se recuperan las bases de datos hasta el punto de error. SnapCenter usa la siguiente secuencia para este proceso:

1. Realiza el backup del último registro de transacciones activo antes de restaurar la base de datos.
2. Restaura las bases de datos desde el backup completo de la base de datos que se seleccione.
3. Aplica todos los registros de transacciones que no estaban comprometidos con las bases de datos (incluidos los registros de transacciones de los backups desde el momento en que se creó el backup hasta el punto más reciente).

   Se mueven los registros de transacciones y se aplican a las bases de datos seleccionadas.

Una operación de restauración de último minuto requiere un conjunto de registros de transacciones contiguos.

Debido a que SnapCenter no puede restaurar registros de transacciones de bases de datos de SQL Server a partir de archivos de backup de envío de registros (el envío de registros permite enviar automáticamente backups de registros de transacciones desde una base de datos principal en una instancia de servidor principal a una o varias bases de datos secundarias en instancias de servidor secundarias independientes), no se puede ejecutar una operación de restauración de último minuto desde los backups de registros de transacciones. Por este motivo, es conveniente usar SnapCenter para realizar el backup de los archivos de registros de transacciones de bases de datos de SQL Server.

Si no se necesita la funcionalidad de restauración de último minuto para todos los backups, es posible configurar la retención de backup de los registros de transacciones del sistema mediante las políticas de backup.

#### Ejemplo de una operación de restauración de último minuto

Supongamos que se ejecuta un backup de SQL Server todos los días al mediodía, y un miércoles a las 4:00 es necesario hacer una restauración desde un backup. Por algún motivo, el backup del miércoles al mediodía no pasó la verificación, por lo que se decide restaurar desde el backup del martes al mediodía. Después de eso, si se restaura el backup, todos los registros de transacciones se mueven hacia adelante y se aplican a

las bases de datos restauradas, a partir de las que no se confirmaron al crear el backup del martes y continuar con el último registro de transacciones escrito el miércoles a las 4:00 (si se realizó el backup de los registros de transacciones).

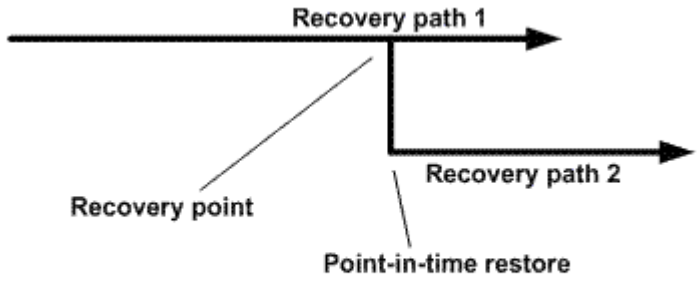
#### Restauración a un momento específico

En una operación de restauración a un momento específico, las bases de datos se restauran únicamente a un punto específico. Esta operación se ejecuta en las siguientes situaciones:

- La base de datos se restaura a un punto específico en un registro de transacciones incluido en un backup.
- Se restaura la base de datos, y solo se aplica un subconjunto de los registros de transacciones del backup.

Cuando se restaura una base de datos a un momento específico, se crea una nueva ruta de recuperación.

En la siguiente imagen, se ilustran los problemas cuando se ejecuta una operación de restauración a un momento específico:




En la imagen, la ruta de recuperación 1 consta de un backup completo seguido por varios backups de registros de transacciones. Se restaura la base de datos a un momento específico. Se crean nuevos backups de registros de transacciones después de la operación de restauración a un momento específico, lo cual da lugar a la ruta de recuperación 2. Se crean nuevos backups de registros de transacciones sin crear un backup completo nuevo. Debido a que hay datos dañados u otros problemas, no es posible restaurar la base de datos actual hasta que se cree un nuevo backup completo. Tampoco es posible aplicar los registros de transacciones creados en la ruta de recuperación 2 al backup completo que pertenece a la ruta de recuperación 1.

Si se aplican backups de registros de transacciones, también es posible especificar una fecha y hora particulares en las que se detendrá la aplicación de las transacciones del backup. Para esto, se especifica una fecha y hora dentro del intervalo disponible, y SnapCenter quita las transacciones que no estuvieran comprometidas antes de ese momento específico. Este método permite restaurar bases de datos a un momento específico antes de que se dañara, o recuperar contenido tras la eliminación accidental de una base de datos o una tabla.

#### Ejemplo de una operación de restauración a un momento específico

Supongamos que se realiza un backup completo de las bases de datos a la medianoche y un backup de los registros de transacciones cada hora. La base de datos falla a las 9:45, pero igual se realiza el backup de los registros de transacciones de la base de datos con errores. Es posible elegir entre las siguientes situaciones de restauración a un momento específico:

- Restaurar el backup completo de las bases de datos de la medianoche y aceptar la pérdida de los cambios hechos posteriormente. (Opción: None).
- Restaurar el backup completo de las bases de datos y aplicar todos los backups de registros de transacciones hasta las 9:45 (Opción: Log until).
- Restaurar el backup completo de las bases de datos y aplicar los backups de registros de transacciones especificando un intervalo de transacciones que se restaurarán del último conjunto de backups de registros de transacciones. (Opción: By specific time).

En este caso, es necesario calcular la fecha y hora en que se informó el error. Las transacciones que no estuvieran comprometidas antes de la fecha y hora especificada se quitan.

## Defina una estrategia de clonación para SQL Server

Definir una estrategia de clonado permite clonar correctamente la base de datos.

1. Revisar las limitaciones de las operaciones de clonado.
2. Decidir el tipo de clon que se necesita.

### Limitaciones de las operaciones de clonado

Antes de clonar las bases de datos, es necesario tener en cuenta las limitaciones de las operaciones de clonado.

- Si utiliza una versión de Oracle de 11.2.0.4 a 12.1.0.1, la operación de clonado estará en estado colgado al ejecutar el comando *renamedg* . Puede aplicar el parche de Oracle 19544733 para solucionar este problema.
- No se admite la clonado de bases de datos de un LUN conectado directamente a un host (por ejemplo, usando el iniciador de iSCSI de Microsoft en un host de Windows) a un VMDK o un LUN de RDM en el mismo host de Windows, ni en otro host de Windows, o viceversa.
- El directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- Si se mueve un LUN que contiene un clon de un volumen nuevo, no es posible eliminar el clon.

### Tipos de operaciones de clonado

Es posible utilizar SnapCenter para clonar un backup de una base de datos de SQL Server o una base de datos de producción.

- Clonación de un backup de base de datos

  La base de datos clonada puede actuar como base de referencia para las aplicaciones y ayudar a aislar errores de la aplicación que se producen en el entorno de producción. La base de datos clonada también puede usarse para la recuperación de errores de la base de datos de software.

- Ciclo de vida de clon

  Es posible utilizar SnapCenter para programar trabajos de clonado recurrentes que se producen cuando la base de datos de producción no está ocupada.

# Inicio rápido de instalar el plugin de SnapCenter para SQL Server

Ofrece un conjunto condensado de instrucciones de instalación para instalar SnapCenter Server y el plugin de SnapCenter para Microsoft SQL Server.

## Preparación de la instalación

### Requisitos de dominio y grupo de trabajo

SnapCenter Server se puede instalar en sistemas que estén en un dominio o en un grupo de trabajo.

Si utiliza un dominio de Active Directory, debe utilizar un usuario de dominio con derechos de administrador local. El usuario de dominio debe ser miembro del grupo de administrador local en el host de Windows.

Si utiliza grupos de trabajo, debe utilizar una cuenta local con derechos de administrador locales.

### Requisitos de licencia

El tipo de licencia que instale dependerá del entorno.

| Licencia | Donde se la requiere |
| --- | --- |
| Basado en controladora estándar de SnapCenter | Necesario para las controladoras de almacenamiento FAS o AFF<br><br>La licencia estándar de SnapCenter es una licencia basada en la controladora y se incluye como parte del paquete Premium. Si tiene la licencia de conjunto de SnapManager, también obtendrá el derecho de licencia estándar de SnapCenter. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS o AFF, puede obtener una licencia de evaluación Premium Bundle poniéndose en contacto con el representante de ventas. |
| SnapCenter basada en capacidad estándar | Necesario con ONTAP Select y Cloud Volumes ONTAP<br><br>Si es cliente de Cloud Volumes ONTAP o ONTAP Select, necesita adquirir una licencia basada en capacidad por TB en función de los datos gestionados por SnapCenter. De forma predeterminada, SnapCenter envía una licencia de prueba integrada basada en capacidad estándar de SnapCenter de 90 días y 100 TB. Si desea obtener más detalles, póngase en contacto con el representante de ventas. |

| Licencia | Donde se la requiere |
| --- | --- |
| SnapMirror o SnapVault | ONTAP<br><br>Se requieren licencias de SnapMirror o SnapVault si la replicación se habilita en SnapCenter. |
| Licencias adicionales (opcional) | Consulte "Licencias SnapCenter". |
| Licencias estándar de SnapCenter (opcional) | Destinos secundarios<br><br>Se recomienda, pero no es obligatorio, añadir licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter están deshabilitadas en destinos secundarios, no puede usar SnapCenter para realizar un backup de los recursos en el destino secundario después de realizar una operación de conmutación al nodo de respaldo. Sin embargo, se requiere una licencia de FlexClone en destinos secundarios para realizar operaciones de clonado y verificación. |

**Requisitos adicionales**

Para ver los requisitos mínimos del ONTAP y el complemento de la aplicación, consulte "Herramienta de matriz de interoperabilidad"

| Hosts | Requisitos mínimos |
| --- | --- |
| Sistema operativo (64 bits) | Consulte "Herramienta de matriz de interoperabilidad" |
| CPU | • Host del servidor: 4 núcleos<br>• Host de plugin: 1 núcleo |
| RAM | • Host del servidor: 8 GB<br>• Host de plugins: 1 GB |

| Hosts | Requisitos mínimos |
| --- | --- |
| Espacio en el disco duro | Host del servidor:<br>• 4 GB para software y registros de SnapCenter Server<br>• 6 GB para el repositorio de SnapCenter<br>• Cada host de plugin: 2 GB para la instalación y los registros de un plugin, esto es obligatorio solo si el plugin está instalado en un host dedicado. |
| Bibliotecas de terceros | Requerida en el host de servidor de SnapCenter y el host de plugins:<br>• Microsoft .NET Framework 4.5.2 o posterior<br>• Windows Management Framework (WMF) 4.0 o posterior<br>• PowerShell 4.0 o posterior |
| Exploradores | Chrome, Internet Explorer y Microsoft Edge |

| Tipo de puerto | Puerto predeterminado |
| --- | --- |
| Puerto SnapCenter | 8146 (HTTPS), bidireccional, personalizable, como en la URL *https://server:8146* |
| Puerto de comunicación SMCore de SnapCenter | 8145 (HTTPS), bidireccional, personalizable |
| Base de datos del repositorio | 3306 (HTTPS), bidireccional |
| Hosts de plugins de Windows | 135 DE FEBRERO DE 445 (TCP)<br>Además de los puertos 135 y 445, el intervalo de puertos dinámico especificado por Microsoft también debería estar abierto. Operaciones de instalación remota Utilice el servicio Instrumental de administración de Windows (WMI), que busca dinámicamente este intervalo de puertos.<br>Para obtener información sobre el intervalo de puertos dinámicos admitido, consulte "Descripción general del servicio y requisitos de puertos de red para Windows". |
| Plugin de SnapCenter para Windows | 8145 (HTTPS), bidireccional, personalizable |

| Tipo de puerto | Puerto predeterminado |
| --- | --- |
| Puerto de comunicación del clúster de ONTAP o de SVM | 443 (HTTPS), bidireccional; 80 (HTTP), bidireccional<br><br>El puerto se utiliza para establecer la comunicación entre el host del servidor de SnapCenter, el host del plugin y SVM o el clúster de ONTAP. |

**Requisitos del complemento SnapCenter para Microsoft SQL Server**

Debe tener un usuario con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto. Si gestiona nodos de clúster, necesita un usuario con privilegios de administrador para todos los nodos del clúster.

Debe tener un usuario con permisos de administrador del sistema en SQL Server. El plugin utiliza Microsoft VDI Framework, para lo que se requiere acceso de sysadmin.

Si utilizaba SnapManager para Microsoft SQL Server y desea importar datos de SnapManager para Microsoft SQL Server a SnapCenter, consulte "Importación de backups archivados"

## Instale el servidor SnapCenter

### Descargue e instale el servidor SnapCenter

- Pasos*

1. Descargue el paquete de instalación del servidor SnapCenter desde el "Sitio de soporte de NetApp" y, a continuación, haga doble clic en el archivo exe.

   Tras iniciar la instalación, se realizan todas las comprobaciones previas y si los requisitos mínimos no son los correctos, se muestran mensajes de error o de advertencia. Puede ignorar los mensajes de advertencia y continuar con la instalación; sin embargo, los errores deben corregirse.

2. Revise los valores rellenados previamente necesarios para la instalación del servidor SnapCenter y modifíquelos si es necesario.

   No es necesario especificar la contraseña para la base de datos de repositorio del servidor MySQL. Durante la instalación del servidor SnapCenter, la contraseña se genera automáticamente.

   El carácter especial “%” no se admite en la ruta personalizada para la instalación. Si incluye “%” en la ruta, la instalación falla.

1. Haga clic en **instalar ahora**.

### Iniciar sesión en SnapCenter

- Pasos*

1. Inicie SnapCenter desde un acceso directo en el escritorio del host o desde la dirección URL proporcionada por la instalación (*https://server:8146* para el puerto predeterminado 8146 donde está instalado SnapCenter Server).
2. Introduzca las credenciales.

Para un formato de nombre de usuario de administrador de dominio integrado, utilice: *NetBIOS\<username>* o *<username>@<domain>* o *<DomainFQDN>\<username>*.

Para un formato de nombre de usuario de administrador local integrado, utilice *<username>*.

1. Haga clic en **Iniciar sesión**.

**Agregar una licencia estándar basada en controlador SnapCenter**

- Pasos*
  1. Inicie sesión en la controladora con la línea de comandos de ONTAP e introduzca lo siguiente:

     ```
     system license add -license-code <license_key>
     ```

  2. Compruebe la licencia:

     ```
     license show
     ```

**Agregar una licencia basada en capacidad de SnapCenter**

- Pasos*
  1. En el panel izquierdo de la GUI de SnapCenter, haga clic en **Configuración > Software** y, a continuación, en la sección Licencia, haga clic en **+**.
  2. Seleccione uno de los dos métodos para obtener la licencia:
     - Introduzca sus credenciales de inicio de sesión en el sitio de soporte de NetApp para importar licencias.
     - Desplácese hasta la ubicación del archivo de licencia de NetApp y haga clic en **Open**.
  3. En la página **Notificaciones** del asistente, utilice el umbral de capacidad predeterminado del 90 por ciento.
  4. Haga clic en **Finalizar**.

**Configurar las conexiones del sistema de almacenamiento**

- Pasos*
  1. En el panel izquierdo, haga clic en **sistemas de almacenamiento > Nuevo**.
  2. En la página Add Storage System, realice lo siguiente:
     a. Introduzca el nombre o la dirección IP del sistema de almacenamiento.
     b. Introduzca las credenciales que se utilizan para acceder al sistema de almacenamiento.
     c. Active las casillas para habilitar el sistema de gestión de eventos (EMS) y AutoSupport.
  3. Haga clic en **más opciones** si desea modificar los valores predeterminados asignados a la plataforma, el protocolo, el puerto y el tiempo de espera.
  4. Haga clic en **Enviar**.

## Instale el plugin para Microsoft SQL Server

**Configurar credenciales Run as para instalar el Plug-in para Microsoft SQL Server**

- Pasos*

1. En el panel izquierdo, haga clic en **Configuración > credenciales > Nuevo**.
2. Introduzca las credenciales.

   Para un formato de nombre de usuario de administrador de dominio integrado, utilice: *NetBIOS\<username>* o *<username>@<domain>* o *<DomainFQDN>\<username>*.

Para un formato de nombre de usuario de administrador local integrado, utilice *<username>*.

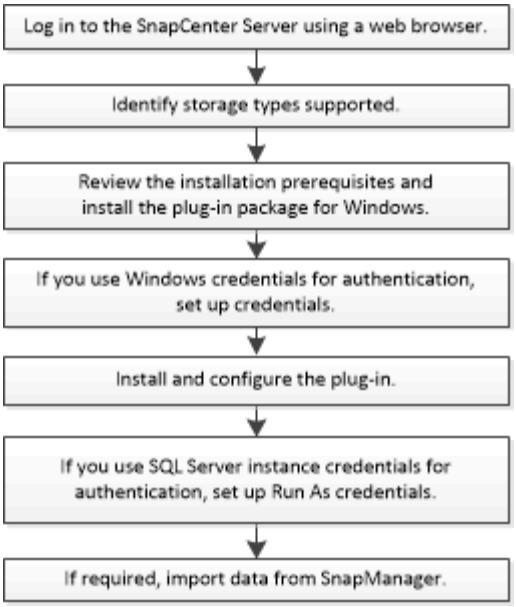
**Agregue un host e instale el plugin para Microsoft SQL Server**

- Pasos*
  1. En el panel izquierdo de la interfaz gráfica de usuario de SnapCenter, haga clic en **hosts > Managed hosts > Add**.
  2. En la página hosts del asistente, realice lo que sigue:
     a. Host Type: Seleccione el tipo de host Windows.
     b. Nombre de host: Utilice el host SQL o especifique el FQDN de un host Windows dedicado.
     c. Credenciales: Seleccione el nombre de credencial válido del host que creó o cree nuevas credenciales.
  3. En la sección Select Plug-ins to Install, seleccione **Microsoft SQL Server**.
  4. Haga clic en **más opciones** para especificar los siguientes detalles:
     a. Puerto: Conserve el número de puerto predeterminado o especifique el número de puerto.
     b. Ruta de instalación: La ruta predeterminada es *C:\Program Files\NetApp\SnapCenter*. Opcionalmente, puede personalizar la ruta.
     c. Añadir todos los hosts del clúster: Seleccione esta casilla de comprobación si está usando SQL en WSFC.
     d. Skip preinstall checks: Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente o no desea validar si el host cumple los requisitos para instalar el plugin.
  5. Haga clic en **Enviar**.

# Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server

## Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft SQL Server

Tendrá que instalar y configurar el plugin de SnapCenter para Microsoft SQL Server si desea proteger las bases de datos de SQL Server.




## Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft SQL Server

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Debe tener un usuario con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Si gestiona nodos de clúster en SnapCenter, debe tener un usuario con privilegios de administrador para todos los nodos del clúster.
- Debe tener un usuario con permisos de administrador del sistema en SQL Server.

  El plugin de SnapCenter para Microsoft SQL Server utiliza Microsoft VDI Framework, para lo que se requiere acceso de sysadmin.

  "Artículo de soporte de Microsoft 2926557: Las operaciones de backup y restauración de VDI de SQL Server requieren privilegios de administrador del sistema"

- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Si está instalado SnapManager para Microsoft SQL Server, debe haber detenido o deshabilitado el servicio y las programaciones.

  Si prevé importar tareas de backup o clonado a SnapCenter, no desinstale SnapManager para Microsoft SQL Server.

- El host debe poder resolverse con el nombre de dominio completo (FQDN) del servidor.

  Si el archivo hosts se modifica para que pueda resolverse y si se especifican tanto el nombre corto como el FQDN en el archivo hosts, cree una entrada en el archivo hosts SnapCenter con el siguiente formato: <ip_address> <host_fqdn> <host_name>

## Configure credenciales para el paquete de plugins de SnapCenter para Windows

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar los plugins de SnapCenter, y credenciales adicionales para realizar operaciones de protección de datos en sistemas de archivos Windows o bases de datos.

**Lo que necesitará**

- Debe configurar credenciales de Windows antes de instalar plugins.
- Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.
- Autenticación SQL en hosts Windows

  Debe configurar credenciales de SQL después de instalar plugins.

  Si va a implementar el plugin de SnapCenter para Microsoft SQL Server, debe configurar las credenciales de SQL después de instalar plugins. Configure una credencial para un usuario con permisos de administrador del sistema en SQL Server.

  El método de autenticación de SQL se verifica de acuerdo con una instancia de SQL Server. Esto significa que debe detectarse una instancia de SQL Server en SnapCenter. Por lo tanto, antes de añadir una credencial de SQL, debe añadir un host, instalar paquetes de plugins y actualizar los recursos. Se necesita la autenticación de SQL Server para realizar operaciones como la programación o la detección de recursos.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página **Configuración**, haga clic en **credenciales**.
  3. Haga clic en **Nuevo**.
  4. En la página **Credential**, especifique la información necesaria para configurar las credenciales:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de credencial | Escriba un nombre para la credencial. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario/Contraseña | Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.<br>• Administrador del dominio<br>Especifique el administrador de dominio en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>• Administrador local (sólo para grupos de trabajo)<br>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: `UserName`<br>No utilice comillas dobles (") ni marcas de retroceso (') en las contraseñas. No debe usar el signo menos de (<) y el signo de exclamación (!) los símbolos juntos en las contraseñas. Por ejemplo, arrendhan<!10, les10<!, backtick'12. |
| Modo de autenticación | Seleccione el modo de autenticación que desea utilizar. Si selecciona el modo de autenticación de SQL, también debe especificar la instancia de SQL Server y el host donde está ubicada esa instancia. |

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede que desee asignar mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

## Configure las credenciales para un recurso individual de SQL Server

Es posible configurar credenciales para realizar trabajos de protección de datos en un recurso individual de SQL Server para cada usuario. Si bien es posible configurar las

credenciales de manera global, se recomienda hacerlo solo para un recurso particular.

**Acerca de esta tarea**

- Si utiliza credenciales de Windows para la autenticación, debe configurar las credenciales para poder instalar plugins.

  Sin embargo, si utiliza una instancia de SQL Server para la autenticación, debe añadir la credencial después de instalar los plugins.

- Si ha habilitado la autenticación SQL durante la configuración de las credenciales, la instancia o base de datos detectadas se mostrarán con un icono de candado de color rojo.

  Si aparece el icono de candado, debe especificar las credenciales de la instancia o la base de datos para añadir correctamente la instancia o la base de datos al grupo de recursos.

- Debe asignar la credencial a un usuario de control de acceso basado en roles (RBAC) sin acceso de administrador del sistema cuando se cumplan las siguientes condiciones:
  - La credencial se asigna a una instancia de SQL.
  - La instancia o el host de SQL se asignan a un usuario de RBAC.

    El usuario debe tener privilegios de backup y grupo de recursos

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página **Configuración**, haga clic en **credenciales**.
  3. Para agregar una nueva credencial, haga clic en **Nuevo**.
  4. En la página **Credential**, configure las credenciales:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Nombre de credenciales** | Introduzca un nombre para las credenciales. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Nombre de usuario** | Introduzca el nombre de usuario utilizado para autenticación de SQL Server.<br>• El administrador de dominio o cualquier miembro del grupo de administrador especifican el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que está instalando el plugin de SnapCenter. Los formatos válidos para el campo **Nombre de usuario** son:<br>◦ *NetBIOS\Username*<br>◦ *Domain FQDN\Username*<br>• Administrador local (sólo para grupos de trabajo) en los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el complemento SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo **Nombre de usuario** es: *Username* |
| **Contraseña** | Introduzca la contraseña usada para autenticación. |
| **Modo de autenticación** | Seleccione el modo de autenticación SQL Server. También es posible seleccionar la autenticación de Windows si el usuario de Windows tiene privilegios de administrador del sistema en el servidor SQL. |
| **Host** | Seleccione el host. |
| **Instancia de SQL Server** | Seleccione la instancia de SQL Server. |

5. Haga clic en **Aceptar** para agregar la credencial.
6. En el panel de navegación de la izquierda, haga clic en **Recursos**.
7. En la página **Recursos**, seleccione **instancia** en la lista **Ver**.
   a. Haga clic en y, a continuación, seleccione el nombre de host para filtrar las instancias.
   b. Haga clic en para cerrar el panel de filtros.
8. En la página **Instance Protect**, proteja la instancia y, si es necesario, haga clic en **Configurar credenciales**.

Si el usuario que ha iniciado sesión en el servidor SnapCenter no tiene acceso al complemento SnapCenter para Microsoft SQL Server, el usuario deberá configurar las credenciales.

La opción de credencial no se aplica a las bases de datos y los grupos de disponibilidad.

1. Haga clic en **Actualizar recursos**.

## Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

**Lo que necesitará**

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

1. Asigne los privilegios administrativos al GMSA configurado en el host.
2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

   El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

## Instale el plugin de SnapCenter para Microsoft SQL Server

### Añada hosts e instale el paquete de plugins de SnapCenter para Windows

Debe utilizar la página SnapCenter **Add Host** para añadir hosts e instalar el paquete de plugins. Los plugins se instalan automáticamente en hosts remotos.

#### Lo que necesitará

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada, deberá deshabilitar UAC en el host.
- Debe asegurarse de que el servicio de cola de mensajes esté en estado en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configurar la cuenta de servicio administrado de grupo en Windows Server 2012 o posterior para SQL"

### Acerca de esta tarea

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

Puede añadir un host e instalar los paquetes de los plugins para un host individual o para un clúster. Si está instalando los plugins en un clúster o clustering de conmutación al nodo de respaldo de Windows Server (WSFC), los plugins se instalan en todos los nodos del clúster.

Para obtener información sobre la gestión de los hosts, consulte "Gestionar hosts".

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página **hosts** haga lo siguiente:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Tipo de host | Seleccione Windows como tipo de host. El servidor de SnapCenter añade el host e instala el plugin para Windows si el plugin todavía no está instalado en el host.<br><br>Si selecciona la opción de Microsoft SQL Server en la página Plug-ins, SnapCenter Server instala el plugin para SQL Server. |
| Nombre de host | Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. La dirección IP es compatible con hosts de dominio que no son de confianza solo si se resuelve en el FQDN.<br><br>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.<br><br>Puede introducir las direcciones IP o el FQDN de uno de los siguientes:<br><br>• Host independiente<br>• WSFC Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar el FQDN. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Credenciales | Seleccione el nombre de credencial que ha creado o cree nuevas credenciales. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales.<br><br>Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado.<br><br>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. |

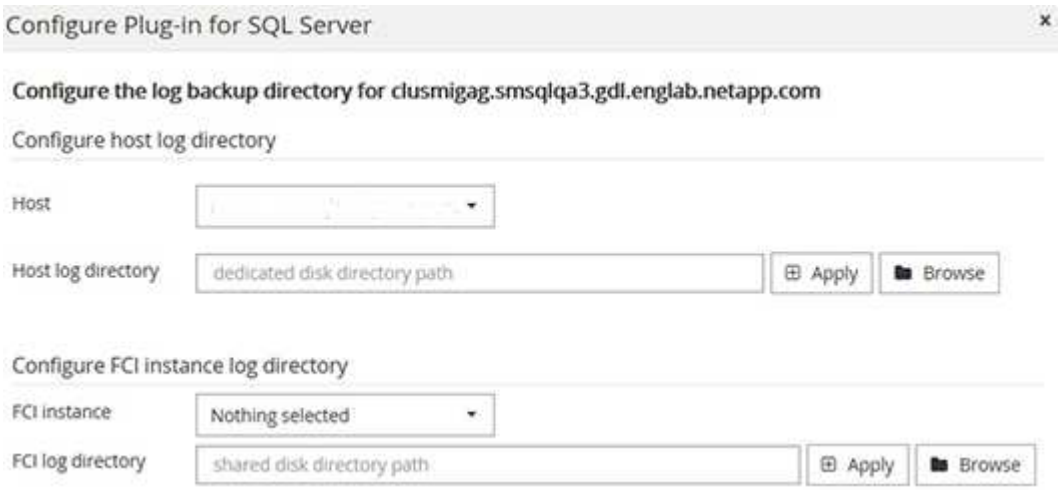
5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.
6. Haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. |
| Ruta de instalación | La ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta. |
| Añada todos los hosts del clúster | Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un WSFC o un Availability Group de SQL. Debe añadir todos los nodos del clúster seleccionando la casilla de comprobación correspondiente del clúster en la GUI si desea gestionar e identificar varios grupos de disponibilidad SQL disponibles en un clúster. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Omitir comprobaciones previas a la instalación | Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin. |
| Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in | Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de complemento.<br><br>Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$.<br><br>Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador de sistema, el GMSA se utilizará para conectarse a la instancia de SQL. |

7. Haga clic en **Enviar**.
8. Para el plugin de SQL, seleccione el host para configurar el directorio de registro.
   a. Haga clic en **Configurar directorio de registro** y en la página **Configurar directorio de registro de host**, haga clic en **examinar** y complete los pasos siguientes:

      Tan solo se enumeran las unidades NetApp LUN como disponibles para su selección. SnapCenter realiza un backup y replica el directorio de registro del host como parte de la operación de backup.




      i. Seleccione la letra de la unidad o el punto de montaje del host donde se almacenará el registro del host.
      ii. Si es necesario, elija un subdirectorio.
      iii. Haga clic en **Guardar**.
9. Haga clic en **Enviar**.

Si no ha seleccionado la casilla de comprobación **Skip prechecks**, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en C:\Program Files\NetApp\SnapCenter WebApp para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero debe solucionar el problema.

En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

1. Supervise el progreso de la instalación.

#### Instale el plugin de SnapCenter para Microsoft SQL Server en varios hosts remotos mediante cmdlets

Puede instalar el plugin de SnapCenter para Microsoft SQL Server en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

**Lo que necesitará**

Debe haberse registrado en SnapCenter como usuario del dominio con derechos de administrador local en cada host en el que desee instalar el paquete de plugins.

- Pasos*

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
3. Instale el plugin de SnapCenter para Microsoft SQL Server en varios hosts remotos mediante el cmdlet Install-SmHostPackage y los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Puede utilizar la opción -skipprecheck cuando ya haya instalado los plugins manualmente y no desee validar si el host cumple los requisitos para instalar el plugin.

1. Introduzca sus credenciales para la instalación remota.

#### Instale el plugin de SnapCenter para Microsoft SQL Server silenciosamente desde la línea de comandos

Debe instalar el plugin de SnapCenter para Microsoft SQL Server desde la interfaz de usuario de SnapCenter. Sin embargo, si no puede hacerlo por algún motivo, puede ejecutar el programa de instalación del plugin para SQL Server sin supervisión en el modo silencioso desde la línea de comandos de Windows.

**Lo que necesitará**

- Debe eliminar la versión anterior del plugin de SnapCenter para Microsoft SQL Server antes de instalar.

  Para obtener más información, consulte "Cómo instalar un plugin de SnapCenter de forma manual y directa desde el host del plugin".

- Pasos*

  1. Compruebe si existe una carpeta C:\temp en el host del plugin y el usuario que ha iniciado sesión tiene acceso completo a ella.
  2. Descargue el software del plugin para SQL Server desde C:\ProgramData\NetApp\SnapCenter\Package Repository.

     Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.
  3. Copie el archivo de instalación en el host en el que desea instalar el plugin.
  4. Desde el símbolo del sistema de Windows en el host local, desplácese hasta el directorio en el que guardó los archivos de instalación del plugin.
  5. Instale el software del plugin para SQL Server:

     ```
     "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
     /log"Log_Path" BI_SNAPCENTER_PORT=Num
     SUITE_INSTALLDIR="Install_Directory_Path"
     BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
     ISFeatureInstall=SCW,SCSQL
     ```

     Sustituya los valores del marcador de posición por sus datos

     - Debug_Log_Path es el nombre y la ubicación del archivo de registro del instalador de la suite.
     - Log_Path es la ubicación de los registros de instalación de los componentes del plugin (SCW, SCSQL y SMCore).
     - Num es el puerto en el que SnapCenter se comunica con SMCore
     - Install_Directory_Path es el directorio de instalación del paquete de plugins del host.
     - Domain\Administrator es la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
     - La contraseña es la contraseña de la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
       ```
       "snapcenter_windows_host_plugin.exe"/silent
       /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
       SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
       BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
       ISFeatureInstall=SCW,SCSQL
       ```

     Todos los parámetros que se pasan durante la instalación del plugin para SQL Server distinguen entre mayúsculas y minúsculas.

  1. Supervise el programador de tareas de Windows, el archivo de registro de instalación principal C:\Installdebug.log y los archivos de instalación adicionales en C:\Temp.
  2. Supervise el directorio %temp% para comprobar que los msiexe.exe instaladores están instalando el software sin errores.

La instalación del plugin para SQL Server registra el plugin en el host y no en el servidor de SnapCenter. Es posible registrar el plugin en SnapCenter Server. Para ello, se debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Una vez añadido el host, el plugin se detecta automáticamente.

### Supervise el estado de la instalación del plugin para SQL Server

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

#### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de instalación.
     e. Haga clic en **aplicar**.
  4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configurar certificado de CA

### Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

### Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

- Pasos*

1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
2. En la ventana **Agregar o quitar complementos**, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
3. En la ventana del complemento **certificados**, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
|---|---|
| Importar clave privada | Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**. |
| Importar formato de archivo | No realice cambios; haga clic en **Siguiente**. |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |
| Finalización del Asistente para importación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación. |

El certificado de importación debe incluirse con la clave privada (los formatos admitidos son: *.pfx, *.p12, *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

### Obtenga la huella digital del certificado de CA

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

- Pasos*
  1. Realice lo siguiente en la interfaz gráfica de usuario:
     a. Haga doble clic en el certificado.
     b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
     c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
     d. Copie los caracteres hexadecimales del cuadro.
     e. Quite los espacios entre los números hexadecimales.

        Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".
  2. Realice lo siguiente desde PowerShell:
     a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

        *Get-ChildItem -Path Cert:\LocalMachine\My*

     b. Copie la huella digital.

### Configure el certificado de CA con servicios de plugins de host de Windows

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

- Pasos*
  1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

     Por ejemplo:

     ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
     . Enlace el certificado recientemente instalado con los servicios de
     plugins del host de Windows mediante la ejecución de los siguientes
     comandos:
     ```

     ```
     > $cert = "<certificate thumbprint>"
     ```

     ```
     > $guid = [guid]::NewGuid().ToString("B")
     ```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
```

Por ejemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

### Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

### Lo que necesitará

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

### Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

## Importe los backups archivados de SnapManager para Microsoft SQL Server a SnapCenter

### Información general sobre la importación de backups archivados

Importar datos de SnapManager para Microsoft SQL Server a SnapCenter le permite continuar utilizando sus datos de versiones anteriores. Puede importar solo los backups que se hayan archivado mediante la tecnología de SnapVault de SnapManager para Microsoft SQL Server a SnapCenter.

SnapCenter no es compatible con Data ONTAP operando en 7-Mode. Puede utilizar la 7-Mode Transition Tool para migrar datos y configuraciones que se almacenan en un sistema que ejecuta Data ONTAP operando en 7-Mode a un sistema ONTAP.

### Limitaciones relacionadas con la función de importación

Si se comprenden las limitaciones antes de importar backups archivados de SnapManager para Microsoft SQL Server en SnapCenter, resulta más sencillo completar la importación correctamente. Estos backups deben haberse archivado con la tecnología SnapVault.

- No puede gestionar clones creados con SnapManager para Microsoft SQL Server en SnapCenter. Debe gestionar los clones en SnapManager para Microsoft SQL Server.
- No puede importar backups desde la interfaz de usuario gráfica de SnapCenter.
- No es posible importar bases de datos desde una máquina virtual con un disco VMDK.

### Importación de backups archivados

Puede importar solo los backups que se han archivado mediante la tecnología de SnapVault de SnapManager para Microsoft SQL Server a SnapCenter desde la interfaz de la línea de comandos.

#### Lo que necesitará

- Tanto el plugin de SnapCenter para Microsoft SQL Server como SnapManager para Microsoft SQL Server 7.x tienen que estar instalados en el mismo host.
- Para que el clúster sea compatible, tanto el plugin como el producto 7.x tienen que haberse instalado en cada nodo del clúster.
- Tiene que haber agregado el host o el clúster a SnapCenter y conocer los recursos disponibles para el backup en el host o el clúster.
- Tiene que haber realizado el backup de la carpeta SnapInfo de SnapManager para Microsoft SQL Server.

  Si la operación de importación fracasa, puede recuperar los metadatos del backup del directorio SnapInfo.

**Práctica recomendada:** es recomendable configurar la carpeta de copia de seguridad de registros para el complemento SnapCenter para Microsoft SQL Server.

Para obtener información acerca de las tareas de instalación y configuración de SnapCenter, consulte la

información de instalación de SnapCenter. Para obtener información acerca de las tareas de instalación y configuración de SnapManager para Microsoft SQL Server, consulte la información de instalación de SnapManager.

Una vez importados los backups archivados a SnapCenter desde SnapManager para Microsoft SQL Server, podrá realizar las operaciones de restauración y clonado en los backups en cuestión desde SnapCenter. Además, podrá continuar realizando simultáneamente operaciones de backup, restauración y clonado usando SnapManager para Microsoft SQL Server.

- Pasos*
  1. Realice los pasos siguientes para crear programaciones de modo similar a cómo SnapManager para Microsoft SQL Server realiza las programaciones manualmente en SnapCenter:
     a. Recupere la información de la programación de SnapManager para Microsoft SQL Server mediante el `Get-SmSchedule` cmdlet.
     b. Guarde la información de la programación.

        Puede utilizar esta información de programación mientras crea políticas en SnapCenter.

     c. Deshabilite las programaciones de SnapManager para Microsoft SQL Server mediante el `Get-SmSchedule -Hostname <hostname> -PluginCode SMSQL -DisableCurrentGenSchedule` cmdlet.
  2. Importe las copias de seguridad archivadas mediante el `Invoke-SmBackupMigration` cmdlet.

**Vea los backups importados en SnapCenter Server**

Después de importar las copias de seguridad archivadas de SnapManager for Microsoft SQL Server, puede ver estas copias de seguridad en SnapCenter desde la página **Topología**.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Cree un grupo de recursos con todas las bases de datos.
  3. Seleccione el grupo de recursos.
  4. Proteja el grupo de recursos.
  5. En la página **Topology**, en la vista **Manage Copies**, haga clic en copias de seguridad de Vault copies.

     Se mostrarán los detalles de los backups.

# Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

### Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

### Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

# Prepárese para la protección de datos

## Requisitos previos para utilizar el plugin de SnapCenter para Microsoft SQL Server

Antes de empezar a utilizar el plugin para SQL Server, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar tareas de requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter.
- Configure el entorno de SnapCenter. Para ello, añada o asigne conexiones de sistema de almacenamiento, y cree credenciales.

  SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada SVM compatible con SnapCenter debe tener un nombre exclusivo.

- Añada hosts, instale los plugins, detecte (actualice) los recursos y configure los plugins.
- Mueva una base de datos de Microsoft SQL Server existente desde un disco local hacia un LUN de NetApp o viceversa ejecutando Invoke-SmConfigureResources.

  Para obtener información sobre cómo ejecutar el cmdlet, consulte "Guía de referencia de cmdlets de SnapCenter Software"

- Si va a utilizar SnapCenter Server para proteger las bases de datos de SQL que residen en LUN o VMDK de VMware RDM, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter. La documentación del plugin de SnapCenter para VMware vSphere tiene más información.

  "Documentación del plugin de SnapCenter para VMware vSphere"

- Ejecutar el aprovisionamiento de almacenamiento en el host mediante el plugin de SnapCenter para Microsoft Windows.
- Mueva las bases de datos existentes al almacenamiento de NetApp.

  Para ver más detalles, consulte la información de importación de SnapCenter.

  "Importe los backups archivados de SnapManager para Microsoft SQL Server a SnapCenter"

- Configure las relaciones de SnapMirror y SnapVault si quiere realizar una replicación de backup.

Para ver más detalles, consulte la información de SnapCenter.

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para los usuarios de SnapCenter 4.3.x, la documentación del plugin de SnapCenter para VMware vSphere 4.3 tiene información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual del plugin de SnapCenter para VMware vSphere basado en Linux (formato de dispositivo virtual abierto).

"Documentación del plugin de SnapCenter para VMware vSphere"

## Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger SQL Server

Antes de usar SnapCenter, es necesariol comprender ciertos conceptos básicos vinculados con las operaciones de backup, clonado y restauración que se ejecutan. El usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos son, por lo general, bases de datos, instancias de bases de datos o grupos de disponibilidad de Microsoft SQL Server que se incluyen en backups o clones con SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupacion de recursos en un host o un clúster.

  Al realizar una operación con un grupo de recursos, esta se ejecuta en los recursos definidos en el grupo de acuerdo con la programación que se especificó para dicho grupo de recursos.

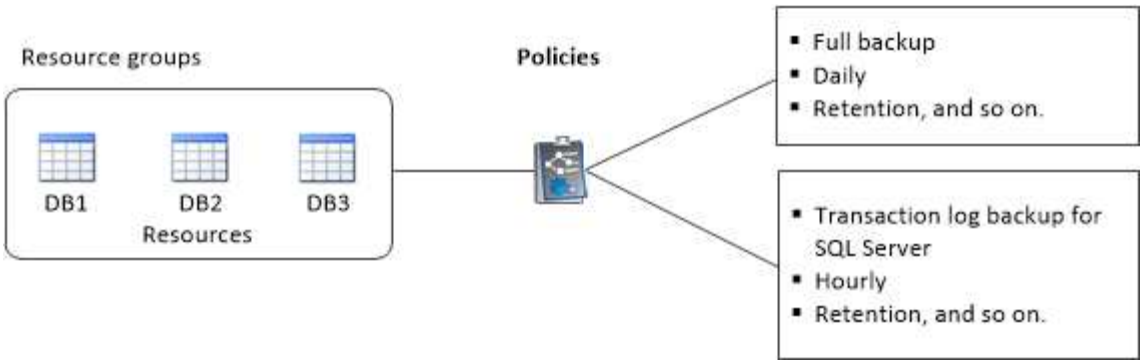
  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

- Las políticas especifican la frecuencia de backup, la retención de copias, la replicación, los scripts y otras características de las operaciones de protección de datos.

  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. Asimismo, puede seleccionar una política al realizar un backup bajo demanda para un recurso individual.

Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos o todos los sistemas de archivos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando se crea el grupo de recursos y se vinculan las políticas, es posible configurar el grupo de recursos para que se ejecute un backup completo todos los días, y agregar una programación que ejecute un backup del registro por hora.

En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:




# Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad

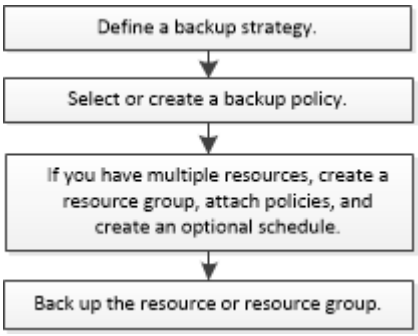
## Flujo de trabajo de backup

Al instalar el plugin de SnapCenter para Microsoft SQL Server en el entorno, puede utilizar SnapCenter para realizar backup de los recursos de SQL Server.

Es posible programar varios backups para que se realicen simultáneamente en diferentes servidores.

No se pueden ejecutar en simultáneo operaciones de backup y restauración en el mismo recurso.

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de backup:




Las opciones Backup Now, Restore, Manage backups y Clone de la página Resources están deshabilitadas si selecciona un LUN que no pertenece a NetApp, una base de datos dañada o una base de datos que se está restaurando.

También puede utilizar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración, recuperación, verificación y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software"

### Cómo SnapCenter hace backups de base de datos

SnapCenter utiliza tecnología de copia de Snapshot para realizar backup de las bases de datos de SQL Server que residen en LUN o VMDK. Para crear el backup, SnapCenter crea copias de Snapshot de las bases de datos.

Cuando se selecciona una base de datos para un backup de base de datos completo en la página Resources,

SnapCenter selecciona automáticamente todas las demás bases de datos que residen en el mismo volumen de almacenamiento. Si el LUN o el VMDK se almacenan en una sola base de datos, puede desactivar o volver a seleccionar la base de datos individualmente. Si el LUN o el VMDK alojan varias bases de datos, debe desactivar o volver a seleccionar las bases de datos como un grupo.

Con las copias de Snapshot, se realiza un backup de todas las bases de datos que residen en un único volumen de forma simultánea. Si el número máximo de bases de datos de backup simultáneo es 35 y residen más de 35 bases de datos en un volumen de almacenamiento, el número total de copias de Snapshot que se crean es igual al número de bases de datos dividido por 35.

Puede configurar el número máximo de bases de datos para cada copia de Snapshot en la política de backups.

Cuando SnapCenter crea una copia de Snapshot, se captura todo el volumen del sistema de almacenamiento en la copia de Snapshot. Sin embargo, el backup solo es válido para el servidor de host SQL para el cual se creó el backup.

Si residen datos de otros servidores de host SQL en el mismo volumen, estos datos no puede restaurarse a partir de la copia de Snapshot.

**Más información**

"Realizar backup de recursos con cmdlets de PowerShell"

"Error de operaciones de inactivación o agrupación de recursos"

## Determine si hay recursos disponibles para backup

Los recursos son las bases de datos, las instancias de aplicaciones, los grupos de disponibilidad y los componentes similares que se mantienen mediante los plugins instalados. Es posible añadir esos recursos a grupos de recursos para ejecutar tareas de protección de datos, pero primero es necesario identificar qué recursos están disponibles. Identificar los recursos disponibles también permite verificar que el plugin se haya instalado correctamente.

**Lo que necesitará**

- Debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts, crear conexiones de sistema de almacenamiento y añadir credenciales.
- Para detectar las bases de datos de Microsoft SQL, se debe cumplir una de las siguientes condiciones.
  - El usuario que se utilizó para añadir el host del plugin a SnapCenter Server debe tener los permisos requeridos (sysadmin) en Microsoft SQL Server.
  - Si no se cumple la condición anterior, en el servidor SnapCenter debe configurar el usuario que tiene los permisos necesarios (sysadmin) en Microsoft SQL Server. El usuario debe configurarse en el nivel de instancia de Microsoft SQL Server y el usuario puede ser un usuario de SQL o Windows.
- Para detectar las bases de datos de Microsoft SQL en un clúster de Windows, debe desbloquear el puerto TCP/IP de la instancia de clúster de conmutación por error (FCI).
- Si las bases de datos residen en LUN o VMDK de VMware, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin en SnapCenter.

  Para obtener más información, consulte "Ponga en marcha el plugin de SnapCenter para VMware

vSphere"

- Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador del sistema, el GMSA se utilizará para conectarse a la instancia de SQL.

**Acerca de esta tarea**

No puede hacer una copia de seguridad de las bases de datos si la opción **Estado general** de la página **Detalles** está configurada en no disponible para la copia de seguridad. La opción **Estado general** se establece en no disponible para copia de seguridad cuando se cumple alguna de las siguientes condiciones:

- Las bases de datos no se encuentran en un LUN de NetApp.
- Las bases de datos no están en estado normal.

  Las bases de datos no se encuentran en el estado normal cuando están sin conexión, en restauración, pendientes de recuperación, suspendidas, etc.

- Las bases de datos tienen privilegios insuficientes.

  Por ejemplo, si un usuario solo tiene acceso para ver la base de datos, no será posible identificar los archivos y las propiedades de la base de datos, por lo que no se podrá realizar un backup.

SnapCenter sólo puede realizar una copia de seguridad de la base de datos primaria si tiene una configuración de grupo de disponibilidad en SQL Server Standard Edition.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Database**, **Instance** o **Availability Group** en la lista desplegable **View**.

     Haga clic en Y seleccione el nombre del host y la instancia de SQL Server para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.

  3. Haga clic en **Actualizar recursos**.

     Los recursos recién agregados, cuyo nombre se ha cambiado o eliminado se actualizan al inventario de SnapCenter Server.

Los recursos se muestran junto con cierta información, como el tipo de recurso, el host o el nombre del clúster, los grupos de recursos asociados, el tipo de backup, las políticas y el estado general.

- Si la base de datos se encuentra en un almacenamiento de terceros, `Not available for backup` Aparece en la columna **Estado general**.

  No es posible ejecutar operaciones de protección de datos en una base de datos que se encuentra en un almacenamiento de terceros.

- Si la base de datos se encuentra en un almacenamiento de NetApp y no está protegida, `Not protected` Aparece en la columna **Estado general**.
- Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, se muestra la interfaz de usuario `Backup not run` Mensaje en la columna **Estado general**.

- Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, y se activa el backup para la base de datos, aparece la interfaz de usuario de `Backup succeeded` Mensaje en la columna **Estado general**.

> Si ha habilitado una autenticación SQL al configurar las credenciales, la instancia o base de datos detectadas se mostrarán con un icono de candado rojo. Si aparece el icono de candado, debe especificar las credenciales de la instancia o la base de datos para añadir correctamente la instancia o la base de datos al grupo de recursos.

Después de que el administrador de SnapCenter asigne los recursos a un usuario de RBAC, el usuario de RBAC debe iniciar sesión y hacer clic en **Actualizar recursos** para ver la última **Estado general** de los recursos.

## Migrar recursos al sistema de almacenamiento de NetApp

Después de haber aprovisionado el sistema de almacenamiento de NetApp con el plugin de SnapCenter para Microsoft Windows, puede migrar los recursos al sistema de almacenamiento de NetApp o de un LUN de NetApp a otro LUN de NetApp mediante la interfaz gráfica de usuario (GUI) de SnapCenter o los cmdlets de PowerShell.

**Lo que necesitará**

- Debe haber añadido sistemas de almacenamiento al servidor SnapCenter.
- Debe haber actualizado (detectado) los recursos de SQL Server.

La mayoría de los campos en estas páginas del asistente son claros y explicativos. La siguiente información describe algunos de los campos que pueden requerir explicación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página **Recursos**, seleccione **base de datos** o **instancia** en la lista desplegable **Ver**.
  3. Seleccione la base de datos o la instancia de la lista y haga clic en **migrar**.
  4. En la página **Recursos**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Nombre de la base de datos** (opcional) | Si ha seleccionado una instancia para la migración, debe seleccionar las bases de datos de esa instancia en la lista desplegable **bases de datos**. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Elija Destinos** | Seleccione la ubicación objetivo para los archivos de datos y de registro.<br><br>Los archivos de datos y de registro se mueven a la carpeta Data and Log correspondiente en la unidad de NetApp seleccionada. Si falta alguna carpeta en la estructura de carpetas, se crea una carpeta y se migra el recurso. |
| **Mostrar detalles del archivo de base de datos** (opcional) | Seleccione esta opción si desea migrar varios archivos de una única base de datos.<br><br>Esta opción no se muestra cuando selecciona el recurso **Instance**. |
| **Opciones** | Seleccione **Delete copy of Migrated Database at original Location** para eliminar la copia de la base de datos del origen.<br><br>Opcional: **EJECUTE ESTADÍSTICAS DE ACTUALIZACIÓN en tablas antes de desvincular la base de datos**. |

5. En la página **Verify**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Opciones de comprobación de consistencia de base de datos** | Seleccione **Ejecutar antes de** para comprobar la integridad de la base de datos antes de la migración. Seleccione **Ejecutar después de** para comprobar la integridad de la base de datos después de la migración. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Opciones de DBCC CHECKDB** | • Seleccione la opción **PHYSICAL_ONLY** para limitar la comprobación de integridad a la estructura física de la base de datos y detectar páginas dañadas, errores de sumas de comprobación y errores de hardware habituales que afecten a la base de datos.<br>• Seleccione la opción **NO_INFOMSGS** para suprimir todos los mensajes informativos.<br>• Seleccione la opción **ALL_ERRORMSGS** para visualizar todos los errores notificados por objeto.<br>• Seleccione la opción **NOINDEX** si no desea comprobar los índices no almacenados en clúster.<br>La base de datos de SQL Server utiliza la comprobación de la consistencia de base de datos de Microsoft SQL Server para comprobar la integridad lógica y física de los objetos de la base de datos.<br>Se recomienda seleccionar esta opción para disminuir el tiempo de ejecución.<br>• Seleccione la opción **TABLOCK** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una copia de Snapshot interna de la base de datos. |

6. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear políticas de backup para bases de datos de SQL Server

Es posible crear una política de backup para el recurso o el grupo de recursos antes de usar SnapCenter con el fin de realizar un backup de los recursos de SQL Server. También es posible crear una política de backup en el momento de crear un grupo de recursos o realizar un backup de un único recurso.

### Lo que necesitará

- Debe estar definida la estrategia de protección de datos.
- Debe haberse preparado para la protección de datos completando ciertas tareas, como instalar SnapCenter, añadir hosts, identificar recursos y crear conexiones con el sistema de almacenamiento.
- Debe haber configurado el directorio de registro del host para backup de registro.
- Debe haber actualizado (detectado) los recursos de SQL Server.

- Si va a replicar copias de Snapshot en un reflejo o almacén, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) para los volúmenes de origen y de destino.

  Para obtener información sobre cómo los administradores asignan recursos a los usuarios, consulte la información de instalación de SnapCenter.

- Si desea ejecutar los scripts de PowerShell en scripts previos y posteriores, debe establecer el valor del parámetro usePowershellProcessforScripts en TRUE en el archivo web.config.

  El valor predeterminado es FALSE

**Acerca de esta tarea**

Una política de backup es un conjunto de reglas que rigen cómo gestionar y conservar backups, y con qué frecuencia se realizará un backup del recurso o del grupo de recursos. De forma adicional, se puede especificar la configuración de replicación y script. Puede especificar opciones en la política para ahorrar tiempo cuando desee reutilizarla con otro grupo de recursos.

La mayoría de los campos en estas páginas del asistente son claros y explicativos. La siguiente información describe algunos de los campos que pueden requerir explicación.

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Directivas**.
  3. Haga clic en **Nuevo**.
  4. En la página **Nombre**, introduzca el nombre y la descripción de la directiva.
  5. En la página **Tipo de copia de seguridad**, realice los siguientes pasos:

     a. Elija el tipo de backup:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Realizar un backup de los archivos de la base de datos y los registros de transacciones, y truncar los registros de transacciones | i. Seleccione **copia de seguridad completa y copia de seguridad de registro**.<br>ii. Introduzca el número máximo de bases de datos que se deben incluir en un backup para cada copia de Snapshot.<br>Debe aumentar dicho valor si desea ejecutar varias operaciones de backup en forma simultánea. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Realice un backup de los archivos de la base de datos | i. Seleccione **copia de seguridad completa**.<br>ii. Introduzca el número máximo de bases de datos que se deben incluir en un backup para cada copia de Snapshot. El valor predeterminado es 100<br>Debe aumentar dicho valor si desea ejecutar varias operaciones de backup en forma simultánea. |
| Realice un backup de los registros de transacciones | Seleccione **copia de seguridad de registro**. |

b. Si va a realizar una copia de seguridad de los recursos mediante otra aplicación de copia de seguridad, seleccione **copia sólo copia de seguridad**.

   Mantener los registros de transacciones intactos permite a cualquier aplicación de backup restaurar la base de datos. Por lo general, no debe utilizar la opción de solo copiar en ningún otro caso.

   Microsoft SQL no es compatible con la opción **copia de seguridad sólo** junto con la opción **copia de seguridad completa y copia de seguridad de registro** para almacenamiento secundario.

c. En la sección Availability Group Settings, realice las siguientes acciones:

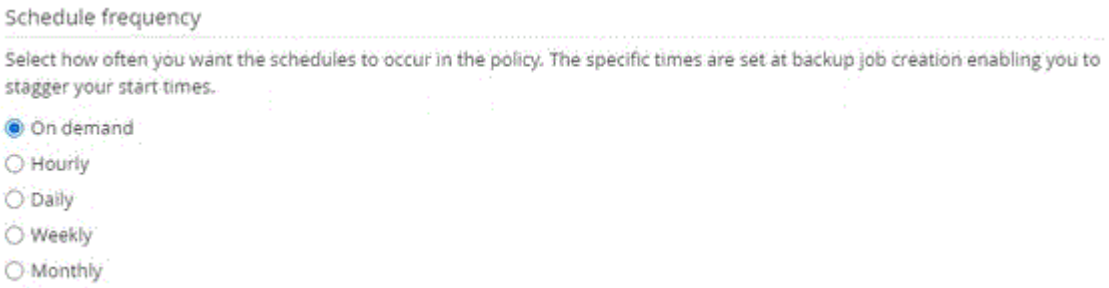
| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Backup solo en réplica de backup preferida | Seleccione esta opción para realizar un backup solo en la réplica de backup preferida. La réplica de backup preferida se decide mediante las preferencias de backup configuradas para el AG en SQL Server. |
| Seleccione réplicas para backup | Seleccione la réplica principal o secundaria del AG para el backup. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Prioridad de backup (prioridad mínima y máxima de backup) | Indique un número mínimo y un número máximo de prioridad de backup mediante los cuales se determine la réplica de AG para backup. Por ejemplo, puede tener una prioridad mínima de 10 y una prioridad máxima de 50. En este caso, se tendrán en cuenta para el backup todas las réplicas de AG que tengan una prioridad superior a 10 e inferior a 50.<br>De forma predeterminada, la prioridad mínima es 1 y la máxima es 100. |

En las configuraciones de clúster, los backups se conservan en cada nodo del clúster según la configuración de retención establecida en la política. Si cambia el nodo propietario del AG, las copias de seguridad se realizan según la configuración de retención y se conservarán las copias de seguridad del nodo propietario anterior. La retención de AG solo se aplica a nivel de nodo.

d. Si desea programar la copia de seguridad que desea crear con esta directiva, especifique el tipo de programa seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

Puede seleccionar un tipo de programación por política.




Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de backup mientras crea un grupo de recursos. De este modo, se pueden crear grupos de recursos que comparten la misma política y frecuencia de backup, pero se pueden asignar diferentes programaciones de backup a cada política.

Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

6. En la página **Retention**, según el tipo de copia de seguridad seleccionado en la página de tipo de copia de seguridad, realice una o más de las siguientes acciones:

a. En la sección Retention settings para la operación de restauración de último minuto, realice una de las siguientes acciones:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Retener únicamente una cantidad específica de copias de Snapshot | Seleccione la opción **Keep log backups aplicable a Last <number> Days** y especifique el número de días que se conservarán. Si se acerca a ese límite, tal vez deba eliminar copias más antiguas. |
| Retener las copias de backup por una cantidad determinada de días | Seleccione la opción **Keep log backups applicable to last <number> days of full backups** y especifique el número de días que se conservarán las copias de seguridad de registros. |

b. En la sección **Configuración de copias de seguridad completas** para la configuración de retención a petición, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Copias de Snapshot totales que se deben conservar | Si desea especificar el número de copias snapshot que desea conservar, seleccione **total Snapshot copies to keep**.<br><br>Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas.<br><br>El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.<br><br>De forma predeterminada, el valor del número de retención se establece en 2. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Conserve copias Snapshot para | Si desea especificar el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas, seleccione **mantener copias Snapshot para**. |

c. En la sección **Configuración de copias de seguridad completas** para las configuraciones de retención por hora, por día, por semana y por mes, especifique la configuración de retención para el tipo de programa seleccionado en la página **Tipo de copia de seguridad**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Copias de Snapshot totales que se deben conservar | Si desea especificar el número de copias snapshot que desea conservar, seleccione **total Snapshot copies to keep**. Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas.<br>Debe establecer el número de retención en 2 o un valor más alto si tiene pensado habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino. |
| Conserve copias Snapshot para | Si desea especificar el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas, seleccione **mantener copias Snapshot para**. |

De forma predeterminada, la retención de copias de Snapshot de registro se establece en 7 días. Use el cmdlet Set-SmPolicy para cambiar la retención de la copia de Snapshot de registro.

En este ejemplo se establece la retención de la copia Snapshot del registro en 2:

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup'
-PluginPolicyType 'SCSQL' -sqlbackuptype 'FullBackupAndLogBackup'
-RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},@{BackupT
ype='LOG_SNAPSHOT';ScheduleType='None';RetentionCount=2},@{BackupType
='LOG';ScheduleType='Hourly';RetentionCount=2} -scheduletype 'Hourly'
```

+
"SnapCenter conserva copias Snapshot de la base de datos"

7. En la página **Replication**, especifique la replicación en el sistema de almacenamiento secundario:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Actualizar SnapMirror tras crear una copia Snapshot local | Seleccione esta opción para crear copias de SnapMirror de conjuntos de backups en otro volumen (SnapMirror). |
| Actualizar SnapVault después de crear una copia Snapshot | Seleccione esta opción para realizar una replicación de backup de disco a disco. |
| Etiqueta de la política secundaria | Seleccione una etiqueta de Snapshot.<br><br>Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta.<br><br>Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria. |
| Número de reintentos con error | Introduzca el número de intentos de replicación que deben producirse antes de que se interrumpa el proceso. |

8. En la página **Script**, introduzca la ruta y los argumentos del script previo o script posterior que se deben ejecutar antes o después de la operación de copia de seguridad, respectivamente.

   Por ejemplo, se puede ejecutar un script para actualizar capturas SNMP, automatizar alertas y enviar registros.

   Debe configurar la política de retención de SnapMirror en ONTAP para que el almacenamiento secundario no alcance el límite máximo de copias de Snapshot.

1. En la página **Verification**, realice los siguientes pasos:
   a. En la sección **Ejecutar verificación para los siguientes programas de copia de seguridad**, seleccione la frecuencia de programación.
   b. En la sección **Opciones de comprobación de consistencia de base de datos**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Limitar la estructura de integridad a la estructura física de la base de datos (PHYSICAL_ONLY) | Seleccione **limitar la estructura de integridad a la estructura física de la base de datos (PHYSICAL_ONLY)** para limitar la comprobación de integridad a la estructura física de la base de datos y detectar páginas dañadas, errores de sumas de comprobación y errores de hardware habituales que afecten a la base de datos. |
| Supress all information messages (NO INFOMSGS) | Seleccione **Supress all information messages (NO INFOMSGS)** para suprimir todos los mensajes informativos. Seleccionado de forma predeterminada. |
| Visualizar todos los mensajes de error notificados por objeto (ALL_ERRORMSGS) | Seleccione **Display all reported error messages per object (ALL_ERRORMSGS)** para visualizar todos los errores notificados por objeto. |
| No comprobar los índices no almacenados en clúster (NOINDEX) | Seleccione **no comprobar los índices no almacenados en clúster (NOINDEX)** si no desea comprobar los índices no almacenados en clúster. La base de datos de SQL Server utiliza la comprobación de la consistencia de base de datos de Microsoft SQL Server para comprobar la integridad lógica y física de los objetos de la base de datos. |
| Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una copia de Snapshot de la base de datos interna (TABLOCK) | Seleccione **Limite las comprobaciones y obtenga los bloqueos en lugar de utilizar una copia de Snapshot de la base de datos interna (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una copia de Snapshot interna de la base de datos. |

c. En la sección **Backup de registro**, seleccione **verificar copia de seguridad de registro al finalizar** para verificar la copia de seguridad de registro al finalizar.

d. En la sección **Verification script settings**, introduzca la ruta de acceso y los argumentos del script previo o posterior que deben ejecutarse antes o después de la operación de verificación, respectivamente.

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear grupos de recursos y asociar políticas para SQL Server

Un grupo de recursos es un contenedor al cual se añaden recursos que se quieren incluir en un backup y proteger en su conjunto. Un grupo de recursos permite realizar un backup en simultáneo de todos los datos que están asociados con una determinada

aplicación. Un grupo de recursos es necesario para cualquier trabajo de protección de datos. También debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

Puede proteger los recursos individualmente sin crear un grupo de recursos nuevo. Puede realizar backups del recurso protegido.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione **base de datos** en la lista **Ver**.

   Si recientemente ha agregado un recurso a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recién añadido.

3. Haga clic en **Nuevo grupo de recursos**.
4. En la página **Nombre**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Nombre | Escriba el nombre del grupo de recursos.<br>El nombre del grupo de recursos no debe superar los 250 caracteres. |
| Etiquetas | Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos. Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta. |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Opcional: Escriba un nombre de copia de Snapshot personalizado y su formato. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |

5. En la página **Recursos**, realice los siguientes pasos:
   a. Seleccione el nombre del host, el tipo de recurso y la instancia de SQL Server en las listas desplegables para filtrar la lista de recursos.

      Si recientemente añadió recursos, aparecerán en la lista Available Resources solo después de actualizar la lista de recursos.

b. Para mover recursos de la sección **Recursos disponibles** a la sección Recursos seleccionados, realice uno de los siguientes pasos:

- Seleccione **Autoselect all resources on same Storage volume** para mover todos los recursos del mismo volumen a la sección Selected Resources.
- Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.

6. En la página **Directivas**, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.

También puede crear una directiva haciendo clic en .

En la sección **Configurar horarios para directivas seleccionadas**, se muestran las directivas seleccionadas.

b. En la sección **Configurar horarios para directivas seleccionadas**, haga clic en En la columna Configure Schedules correspondiente a la directiva para la que desea configurar la programación.

c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación especificando la fecha de inicio, la fecha de caducidad y la frecuencia y, a continuación, haga clic en **Aceptar**.

Debe hacerlo con cada frecuencia que figure en la política. Los horarios configurados se enumeran en la columna Applied Schedules en la sección **Configure schedules for selected policies**.

d. Seleccione Microsoft SQL Server Scheduler.

También debe seleccionar una instancia de programador para asociar con la política de programación.

Si no selecciona Microsoft SQL Server Scheduler, el valor predeterminado es Microsoft Windows Scheduler.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter. No debe modificar las programaciones y cambiar el nombre del trabajo de backup creado en el programador de Windows o el agente de SQL Server.

7. En la página **Verification**, realice los siguientes pasos:

a. Seleccione el servidor de verificación de la lista desplegable **servidor de verificación**.

La lista incluye todos los servidores SQL agregados en SnapCenter. Puede seleccionar varios servidores de verificación (host local o remoto).

La versión del servidor de verificación debe coincidir con la versión y edición del servidor SQL que aloja la base de datos principal.

a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror y SnapVault y realizar la verificación en el almacenamiento secundario.

b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en

.

c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

| Si desea… | Realice lo siguiente… |
|---|---|
| Ejecutar la verificación después del backup | Seleccione **Ejecutar verificación después de la copia de seguridad**. |
| Programar una verificación | Seleccione **Ejecutar verificación programada**. |

d. Haga clic en **Aceptar**.

Las programaciones configuradas figuran en la columna Applied Schedules. Puede revisar y editar haciendo clic en o eliminar haciendo clic en .

8. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

Para habilitar la notificación por correo electrónico, debe tener especificados los detalles del servidor SNMP ya sea mediante la GUI o el comando Set-SmSmtpServer de PowerShell.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

**Más información**

"Crear políticas de backup para bases de datos de SQL Server"

## Requisitos para realizar backups de recursos de SQL

Antes de realizar el backup de un recurso de SQL, debe asegurarse de que se cumplan varios requisitos.

- Debe haber migrado el recurso de un sistema de almacenamiento que no sea de NetApp a un sistema de almacenamiento de NetApp.
- Debe tener creada una política de backup.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Se produce un error en la operación de backup iniciada por un usuario de Active Directory (AD) si la credencial de la instancia de SQL no está asignada al usuario o grupo de AD. Debe asignar la credencial de instancia SQL a un usuario o grupo de AD en la página **Configuración** > **acceso de usuario**.
- Debe tener creado un grupo de recursos con una política anexada.

- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, es posible que la operación de backup en algunos hosts se active tarde debido a problemas de red. Debe configurar el valor de FMaxRetryForUninitializedHosts en web.config con el cmdlet Set-SmConfigSettings de PS.

## Realice backups de recursos de SQL

Si un recurso aún no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

**Acerca de esta tarea**

- Para la autenticación de credenciales de Windows, debe configurar la credencial antes de instalar los plugins.
- Para la autenticación de la instancia de SQL Server, debe añadir la credencial después de instalar los plugins.
- Para la autenticación GMSA, debe configurar GMSA mientras registra el host con SnapCenter en la página **Agregar host** o **Modificar host** para activar y utilizar el GMSA.
- Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador del sistema, el GMSA se utilizará para conectarse a la instancia de SQL.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** ,or **Instance**, o **Availability Group** en la lista desplegable **View**.

   a. Seleccione la base de datos, la instancia o el grupo de disponibilidad que desea incluir en un backup.

      Cuando se realiza el backup de una instancia, la información acerca del último estado de backup o sobre la fecha/hora de esa instancia no están disponibles en la página de recursos.

   En la vista de topología, no puede diferenciar si el estado del backup, la fecha/hora o el backup corresponden a una instancia o a una base de datos.

3. En la página **Recursos**, active la casilla de verificación **Formato de nombre personalizado para copia Snapshot** y, a continuación, escriba un formato de nombre personalizado que desee utilizar para el nombre de copia Snapshot.

   Por ejemplo, customtext_policy_hostname o resource_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.

4. En la página **Directivas**, realice las siguientes tareas:

   a. En la sección **Directivas**, seleccione una o más políticas de la lista desplegable.

      Puede crear una política haciendo clic en para iniciar el asistente de políticas.

      En la sección **Configurar horarios para directivas seleccionadas**, se muestran las directivas seleccionadas.

b. Haga clic en + En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

c. En la sección **Agregar horarios para la directiva** `policy_name` Configure la programación y, a continuación, haga clic en **Aceptar**.

Aquí `policy_name` es el nombre de la política seleccionada.

Los horarios configurados se enumeran en la columna **programas aplicados**.

a. Seleccione **Use Microsoft SQL Server Scheduler** y, a continuación, seleccione la instancia del programador en la lista desplegable **Scheduler Instance** asociada con la directiva de programación.

5. En la página **Verification**, realice los siguientes pasos:

a. Seleccione el servidor de verificación de la lista desplegable **servidor de verificación**.

Puede seleccionar varios servidores de verificación (host local o remoto).

La versión del servidor de verificación debe ser igual o superior a la versión de la edición del servidor SQL que aloja la base de datos principal.

a. Seleccione **cargar localizadores secundarios para verificar copias de seguridad en secundario** para verificar las copias de seguridad en el sistema de almacenamiento secundario.

b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en + .

c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

| Si desea… | Realice lo siguiente… |
|---|---|
| Ejecutar la verificación después del backup | Seleccione **Ejecutar verificación después de la copia de seguridad**. |
| Programar una verificación | Seleccione **Ejecutar verificación programada**. |

Si el servidor de verificación no tiene una conexión de almacenamiento, la operación de verificación genera un error: No se pudo montar el disco.

d. Haga clic en **Aceptar**.

Las programaciones configuradas figuran en la columna Applied Schedules.

6. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

Para habilitar la notificación por correo electrónico, debe tener especificados los detalles del servidor SNMP ya sea mediante la GUI o el comando Set-SmSmtpServer de PowerShell.

7. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de la base de datos.

8. Haga clic en **copia de seguridad ahora**.
9. En la página **copia de seguridad**, realice los siguientes pasos:

   a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Seleccione **verificar después de la copia de seguridad** para verificar la copia de seguridad.
   c. Haga clic en **copia de seguridad**.

      No debe cambiar el nombre del trabajo de backup creado en el programador de Windows o el agente de SQL Server.

   Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

Se crea un grupo de recursos implícito. Puede ver esto seleccionando el usuario o grupo correspondiente en la página **acceso de usuario**. El tipo de grupo de recursos implícito es "'recurso'".

1. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Después de terminar**

- En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

  "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"

- Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup. Para aumentar el tamaño de pila de Java, busque el archivo de script /opt/netapp/init_scripts/scvservice. En ese script, la `do_start method` Command inicia el servicio de plugin de VMware de SnapCenter. Actualice este comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

**Más información**

"Crear políticas de backup para bases de datos de SQL Server"

"Realizar backup de recursos con cmdlets de PowerShell"

"Se produce un error en las operaciones de backup con un error de conexión de MySQL debido a una demora en TCP_TIMEOUT"

"Error de backup con programador de Windows"

"Error de operaciones de inactivación o agrupación de recursos"

## Realizar un backup de grupos de recursos de SQL Server

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Puede buscar el grupo de recursos escribiendo el nombre en el cuadro de búsqueda o haciendo clic en y, a continuación, seleccionar la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. En la página **grupos de recursos**, seleccione el grupo de recursos del que desea realizar la copia de seguridad y, a continuación, haga clic en **realizar copia de seguridad ahora**.
4. En la página **copia de seguridad**, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Después de la copia de seguridad, seleccione **Verify** para verificar la copia de seguridad bajo demanda.

      La opción **verificar** de la directiva sólo se aplica a los trabajos programados.

   c. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Más información**

"Crear políticas de backup para bases de datos de SQL Server"

"Crear grupos de recursos y asociar políticas para SQL Server"

"Realizar backup de recursos con cmdlets de PowerShell"

"Se produce un error en las operaciones de backup con un error de conexión de MySQL debido a una demora en TCP_TIMEOUT"

"Error de backup con programador de Windows"

# Supervisar las operaciones de backup

## Supervise las operaciones de backup de los recursos de SQL en la página SnapCenter Jobs

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Jobs**.
3. En la página Jobs, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
   d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
   e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

   Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

## Supervise las operaciones de protección de datos en recursos de SQL en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también

muestra información sobre la operación de propagación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

     Al hacer clic en una de las operaciones, se muestran sus detalles en la página Job Details.

## Cancelar las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server

Es posible cancelar las operaciones de backup que se ejecutan, se encuentran en cola o no responden. Cuando se cancela una operación de backup, el servidor de SnapCenter detiene la operación y quita todas las copias de Snapshot del almacenamiento si el backup creado no se registra en SnapCenter Server. Si el backup ya está registrado en el servidor SnapCenter, no retrocederá la copia de Snapshot ya creada incluso después de que se active la cancelación.

**Lo que necesitará**

- Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.
- Solo es posible cancelar las operaciones de registro o backup completo que se encuentran en cola o en ejecución.
- No se puede cancelar la operación una vez iniciada la verificación.

  Si cancela la operación antes de verificarlo, se cancelará la operación y no realizará la operación de verificación.
- Es posible cancelar una operación de backup desde la página Monitor o el panel Activity.
- Además de usar la interfaz gráfica de usuario de SnapCenter, es posible usar los cmdlets de PowerShell para cancelar las operaciones.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione el trabajo y haga clic en **Cancelar trabajo** . |

| Del… | Acción |
| --- | --- |
| Panel de actividades | 1. Después de iniciar el trabajo de backup, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

**resultado**

Se cancela la operación y el recurso se revierte al estado anterior. Si la operación que canceló no responde en el estado cancelando o ejecutando, debe ejecutar la `Cancel-SmJob -JobID <int> -Force` cmdlet para detener forzar la operación de backup.

## Consulte los backups y los clones de SQL Server en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario.

**Acerca de esta tarea**

En la página **Topology**, puede ver todas las copias de seguridad y clones disponibles para el recurso o grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Puede consultar los siguientes iconos en la vista **Administrar copias** para determinar si las copias de seguridad y clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o copias vault).

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
- Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.
- Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.
  - La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario.

    Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

Los clones de un backup de un reflejo con versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejo no incluye el backup con versión flexible.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

   Si el recurso seleccionado es una base de datos clonada, protéjala. El origen del clon se muestra en la página Topology. Haga clic en **Detalles** para ver la copia de seguridad utilizada para clonar.

   Si el recurso está protegido, se muestra la página **Topología** del recurso seleccionado.

4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el almacenamiento principal y secundario.

   La sección **Tarjeta de resumen** muestra el número total de copias de seguridad y clones.

Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

1. En la vista **Administrar copias**, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

   Estos detalles se muestran en forma de tabla.

2. Seleccione el backup en la tabla y haga clic en los iconos de protección de datos para realizar operaciones de restauración, clonado, cambio de nombre y eliminación.

   Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

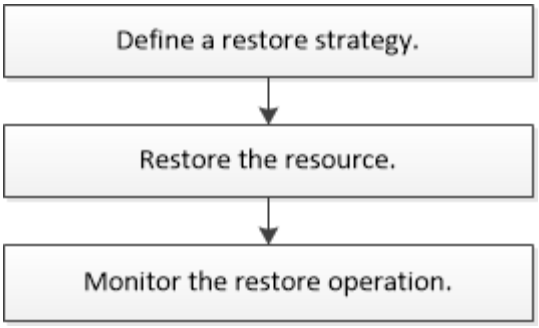
3. Seleccione un clon de la tabla y haga clic en **Clonar división**.
4. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .

# Restaure recursos de SQL Server

## Restaure el flujo de trabajo

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server. Para ello, debe restaurar los datos a partir de uno o más backups en el sistema de archivos activo y, posteriormente, recuperar la base de datos. También puede restaurar las bases de datos que están en grupos de disponibilidad y después añadirlas a esos grupos. Antes de restaurar una base de datos de SQL Server, debe realizar varias tareas preparatorias.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar las operaciones de restauración de bases de datos:




También puede utilizar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración, recuperación, verificación y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlet de SnapCenter Software 4.4"

**Más información**

"Restaurar una base de datos de SQL Server a partir de almacenamiento secundario"

"Restaurar y recuperar recursos con cmdlets de PowerShell"

"Es posible que se produzca un error en la operación de restauración en Windows 2008 R2"

## Requisitos para restaurar una base de datos

Antes de restaurar una base de datos de SQL Server a partir de un backup del plugin de SnapCenter para Microsoft SQL Server, debe asegurarse de que se cumplan diversos requisitos.

- La instancia de SQL Server de destino debe estar en línea y en ejecución para poder restaurar una base de datos.

  Esto se aplica tanto a operaciones de restauración de bases de datos del usuario como a operaciones de restauración de bases de datos del sistema.

- Deben deshabilitarse las operaciones de SnapCenter que están programadas para ejecutarse con los datos de SQL Server que se van a restaurar, lo que incluye cualquier trabajo programado en servidores de gestión remota o de verificación remota.
- Si las bases de datos del sistema no son funcionales, debe reconstruir primero las bases de datos del sistema con una utilidad de SQL Server.
- Si va a instalar el plugin, asegúrese de conceder permisos para que otros roles restauren los backups del grupo de disponibilidad (AG).

  La restauración de AG falla cuando se cumple alguna de las siguientes condiciones:

  - Si el plugin se instala mediante un usuario de RBAC y un administrador intenta restaurar un backup de AG
  - Si el plugin se instala mediante un administrador y un usuario de RBAC intenta restaurar un backup de AG
- Si va a restaurar backups de directorio de registro personalizado en un host alternativo, SnapCenter Server y el host del plugin deben tener instalada la misma versión de SnapCenter.

- Debe tener instalada la revisión KB2887595 de Microsoft. El sitio de asistencia técnica de Microsoft contiene más información acerca de KB2887595.

  "Artículo de soporte de Microsoft 2887595: Paquete acumulativo de actualizaciones de Windows RT 8.1, Windows 8.1 y Windows Server 2012 R2: Noviembre de 2013"

- Debe tener un backup de los grupos de recursos o de las bases de datos.
- Si va a replicar copias de Snapshot en un reflejo o almacén, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) para los volúmenes de origen y de destino.

  Para obtener información sobre cómo los administradores asignan recursos a los usuarios, consulte la información de instalación de SnapCenter.

- Todos los trabajos de backup y clonado deben detenerse antes de restaurar la base de datos.
- Se puede agotar el tiempo de espera de la operación de restauración si el tamaño de la base de datos está en terabytes (TB).

  Aumente el valor del parámetro RESTTimeout de SnapCenter Server a 20000000 ms. Para ello, ejecute el siguiente comando: Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}. Según el tamaño de la base de datos, el valor del tiempo de espera puede cambiarse y el valor máximo que se puede configurar es 2147483648.

Si desea restaurar mientras las bases de datos están en línea, la opción de restauración en línea debe estar habilitada en la página Restore.

## Restaurar backups de base de datos de SQL Server

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server con backup. La restauración de bases de datos es un proceso multifásico que copia todos los datos y las páginas de registro de un backup de SQL Server en una base de datos especificada.

### Acerca de esta tarea

- Puede restaurar las bases de datos de SQL Server con backup en una instancia diferente de SQL Server en el mismo host en que se creó el backup.

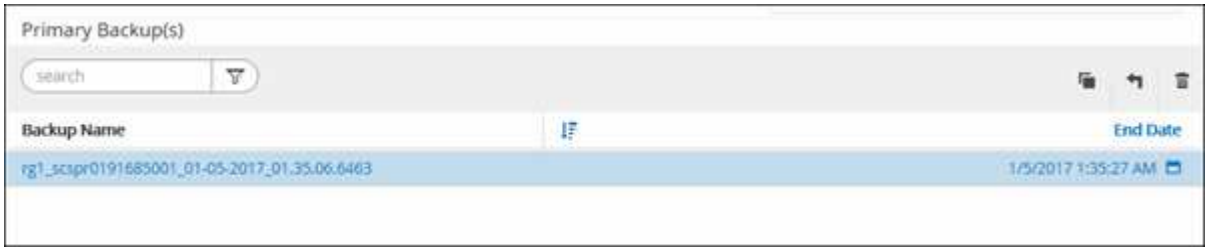
  Puede utilizar SnapCenter para restaurar las bases de datos de SQL Server con backup en una ruta alternativa para no sustituir una versión de producción.

- SnapCenter puede restaurar bases de datos en un clúster de Windows sin que el grupo de clústeres de SQL Server quede sin conexión.
- Si se produce un fallo de clúster (una operación de movimiento de grupos de clústeres) durante una operación de restauración (por ejemplo, si se desactiva el nodo al que pertenecen los recursos), debe volver a conectarse a la instancia de SQL Server y reiniciar la operación de restauración.
- No puede restaurar la base de datos cuando los usuarios o los trabajos de SQL Server Agent acceden a la base de datos.
- No puede restaurar bases de datos del sistema en una ruta alternativa.
- La mayoría de los campos del asistente Restore son claros y explicativos. Aquí se ofrece información sobre los campos que podrían presentar dificultades.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione **base de datos** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione la base de datos o el grupo de recursos en la lista.

   Se muestra la página de topología.

4. En la vista **Administrar copias**, seleccione **copias de seguridad** en el sistema de almacenamiento.
5. Seleccione el backup en la tabla y haga clic en el .




6. En la página **Restore Scope**, seleccione una de las siguientes opciones:

| Opción | Descripción |
|---|---|
| Restaure la base de datos en el mismo host en el que se creó el backup | Seleccione esta opción si desea restaurar la base de datos en la misma instancia de SQL Server donde se realizan los backups. |
| Restaurar la base de datos en un host alternativo | Seleccione esta opción si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o diferente donde se realizan los backups.<br><br>Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración.<br><br>La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original.<br><br>Si la opción **Restaurar la base de datos a un host alternativo** no aparece en la página Restaurar ámbito, borre la memoria caché del explorador. |

| Opción | Descripción |
| --- | --- |
| Restaurar la base de datos con archivos de base de datos existentes | Seleccione esta opción si desea que la base de datos se restaure en un SQL Server alternativo en el mismo host o en otro donde se realizan los backups.<br><br>Los archivos de bases de datos ya deben estar presentes en las rutas de archivos existentes dadas. Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración. |

7. En la página **alcance de recuperación**, seleccione una de las siguientes opciones:

| Opción | Descripción |
| --- | --- |
| Ninguno | Seleccione **Ninguno** cuando necesite restaurar sólo la copia de seguridad completa sin ningún registro. |
| Todos los backups de registros | Seleccione **All log backups** up-to-the-minute backup restore operation para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa. |
| Mediante backups de registros hasta que | Seleccione **by log backups** para realizar una operación de restauración a un momento específico, que restaura la base de datos en función de los registros de copia de seguridad hasta el registro de copia de seguridad con la fecha seleccionada. |
| Por fecha específica hasta | Seleccione **by specific date until** para especificar la fecha y la hora después de las cuales no se aplican registros de transacciones a la base de datos restaurada.<br><br>Esta operación de restauración a un momento específico detiene la restauración de entradas de registro registradas después de la fecha y la hora especificadas. |

| Opción | Descripción |
| --- | --- |
| Utilizar directorio de registro personalizado | Si ha seleccionado **todas las copias de seguridad de registro**, **por copias de seguridad de registro** o **por fecha específica hasta** y los registros se encuentran en una ubicación personalizada, seleccione **usar directorio de registro personalizado** y, a continuación, especifique la ubicación del registro.<br><br>El directorio de registro personalizado no se admite en la base de datos de grupos de disponibilidad. |

8. En la página **Pre OPS**, realice los siguientes pasos:
   a. En la página **Opciones previas a la restauración**, seleccione una de las siguientes opciones:
      - Seleccione **Sobrescribir la base de datos con el mismo nombre durante la restauración** para restaurar la base de datos con el mismo nombre.
      - Seleccione **mantener la configuración de replicación de bases de datos SQL** para restaurar la base de datos y mantener la configuración de replicación existente.
      - Seleccione **Crear copia de seguridad del registro de transacciones antes de restaurar** para crear un registro de transacciones antes de que comience la operación de restauración.
      - Seleccione **Quit restore if transaction log backup before restore fails** para anular la operación de restauración si falla la copia de seguridad del registro de transacciones.
   b. Especifique scripts opcionales que ejecutar antes de realizar un trabajo de restauración.

      Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

9. En la página **Post OPS**, realice los siguientes pasos:
   a. En la sección Choose database state after restore completes, seleccione una de las siguientes opciones:
      - Seleccione **Operational, but unavailable for restoring additional transaction logs** si va a restaurar todas las copias de seguridad necesarias ahora.

        Este es el comportamiento predeterminado, que deja la base de datos preparada para su uso revirtiendo las transacciones no comprometidas. No podrá restaurar registros de transacciones adicionales hasta que cree un backup.

      - Seleccione **no operativo, pero disponible para restaurar registros transaccionales adicionales** para dejar la base de datos no operativa sin revertir las transacciones no comprometidas.

        Pueden restaurarse registros de transacciones adicionales. No podrá utilizar la base de datos hasta que esta se recupere.

      - Seleccione **modo de sólo lectura, disponible para restaurar registros transaccionales adicionales** para dejar la base de datos en modo de sólo lectura.

Esta opción deshace las transacciones no comprometidas, pero guarda las acciones deshechas en un archivo en espera para que puedan revertirse los efectos de recuperación.

Si se habilita la opción Undo directory, se restauran más registros de transacciones. Si la operación de restauración para el registro de transacciones no se realiza correctamente, pueden revertirse los cambios. La documentación de SQL Server contiene más información.

a. Especifique scripts opcionales tras realizar un trabajo de restauración.

   Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

   1. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

      También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo.

   2. Revise el resumen y, a continuación, haga clic en **Finalizar**.
   3. Supervise el proceso de restauración mediante la página **Monitor** > **Jobs**.

**Más información**

"Restaurar y recuperar recursos con cmdlets de PowerShell"

"Restaurar una base de datos de SQL Server a partir de almacenamiento secundario"

## Restaurar una base de datos de SQL Server a partir de almacenamiento secundario

Puede restaurar bases de datos de SQL Server con backup a partir de LUN físicos (RDM, iSCSI o FCP) en un sistema de almacenamiento secundario. La función de restauración es un proceso multifásico que copia todos los datos y las páginas de registro a partir de un backup de SQL Server especificado que reside en el sistema de almacenamiento secundario en una base de datos especificada.

**Lo que necesitará**

- Debe haber replicado las copias de Snapshot a desde el sistema de almacenamiento principal hasta el secundario.
- Debe asegurarse de que SnapCenter Server y el host del plugin puedan conectarse al sistema de almacenamiento secundario.
- La mayoría de los campos del asistente Restore se explican en el proceso de restauración básico. Aquí se ofrece información sobre algunos de los campos que podrían presentar dificultades.
- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **complemento SnapCenter para SQL Server** en la lista.
  2. En la página Resources, seleccione **Database** o **Resource Group** en la lista desplegable **View**.
  3. Seleccione la base de datos o el grupo de recursos.

     Se muestra la página de topología de la base de datos o el grupo de recursos.

4. En la sección Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento secundario (reflejado o almacén).
5. Seleccione el backup en la lista y haga clic en .
6. En la página **ubicación**, elija el volumen de destino para restaurar el recurso seleccionado.
7. Complete el asistente Restaurar, revise el resumen y, a continuación, haga clic en **Finalizar**.

Si restauró una base de datos en una ruta diferente compartida por otras bases de datos, debe realizar un backup completo y una verificación de backup para confirmar que la base de datos restaurada no tiene daños de nivel físico.

## Propagación de bases de datos de grupos de disponibilidad

La propagación es una opción para restaurar las bases de datos de grupos de disponibilidad (AG). Si una base de datos secundaria deja de estar sincronizada con la base de datos principal de un AG, puede propagar la base de datos secundaria.

**Lo que necesitará**

- Debe tener creado un backup de la base de datos de AG secundaria que desea restaurar.
- El servidor de SnapCenter y el host del plugin deben tener instalada la misma versión de SnapCenter.

**Acerca de esta tarea**

- No puede ejecutar la operación de propagación con bases de datos principales.
- No puede realizar una operación de propagación si la base de datos de réplica se quita del grupo de disponibilidad. Cuando se elimina la réplica, la operación de propagación genera un error.
- Mientras ejecuta la operación de propagación con la base de datos de SQL Availability Group, no debe activar los backups de registro en las bases de datos de réplica de esa base de datos de grupo de disponibilidad. Si activa los backups de registros durante la operación de propagación, la operación de propagación con la base de datos de reflejo, "database_name" tiene datos de registro de transacciones insuficientes para preservar la cadena de backup de registros del mensaje de error principal de la base de datos.
- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **complemento SnapCenter para SQL Server** en la lista.
  2. En la página **Recursos**, seleccione **base de datos** en la lista **Ver**.
  3. Seleccione la base de datos secundaria de AG de la lista.
  4. Haga clic en **reseed**.
  5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Supervisar operaciones de restauración de recursos de SQL

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

**Acerca de esta tarea**

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

## Cancelar las operaciones de restauración de recursos de SQL

Es posible cancelar los trabajos de restauración que se encuentran en cola.

Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.

**Acerca de esta tarea**

- Es posible cancelar una operación de restauración en cola desde la página Monitor o el panel Activity.

- No se puede cancelar una operación de restauración en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está desactivado para operaciones de restauración que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de restauración en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
|---|---|
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione el trabajo y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar la operación de restauración, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

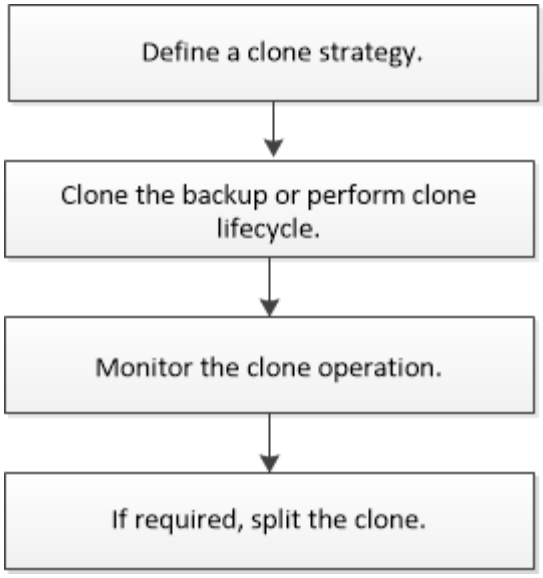
# Clone recursos de bases de datos de SQL Server

## Flujo de trabajo de clonado

Debe ejecutar varias tareas con SnapCenter Server antes de clonar los recursos de bases de datos a partir de un backup. La clonado de base de datos es el proceso de crear una copia de un momento específico de una base de datos de producción o su conjunto de backups. Puede clonar bases de datos para probar la funcionalidad que se debe implementar utilizando la estructura y el contenido actuales de la base de datos durante los ciclos de desarrollo de aplicaciones, para usar las herramientas de extracción y manipulación de datos al rellenar almacenes de datos, o bien ara recuperar datos que se eliminaron o cambiaron por error.

Las operaciones de clonado de bases de datos generan informes basados en los ID de trabajo.

El siguiente flujo de datos muestra la secuencia en la que debe ejecutar las operaciones de clonado:




También puede utilizar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración, recuperación, verificación y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software"

**Más información**

"Clonar a partir de un backup de base de datos de SQL Server"

"Ejecute el ciclo de vida del clon"

"Es posible que la operación de clonado produzca errores o tarde más tiempo en finalizar con el valor TCP_TIMEOUT predeterminado"

## Clonar a partir de un backup de base de datos de SQL Server

Puede utilizar SnapCenter para clonar un backup de base de datos de SQL Server. Si desea acceder a o restaurar una versión anterior de los datos, puede clonar backups de base de datos bajo demanda.

**Lo que necesitará**

- Debe haberse preparado para la protección de datos completando ciertas tareas, como añadir hosts, identificar recursos y crear conexiones de sistema de almacenamiento.
- Debe tener un backup de las bases de datos o de los grupos de recursos.
- El tipo de protección, como reflejo, almacén o reflejo-almacén para el LUN de datos y el LUN de registro, debe ser el mismo para detectar localizadores secundarios durante la clonado en un host alternativo mediante backups de registros.
- Si no se puede encontrar la unidad de clonado montada durante una operación de clonado de SnapCenter, debe cambiar el parámetro CloneRetryTimeout de SnapCenter Server a 300.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).

**Acerca de esta tarea**

- Mientras se clona en una instancia de base de datos independiente, asegúrese de que exista la ruta de acceso del punto de montaje y sea un disco dedicado.
- Al realizar la clonación en una instancia de clúster de conmutación por error (FCI, Failover Cluster Instance), asegúrese de que los puntos de montaje existen, son un disco compartido y la ruta de acceso y el FCI deben pertenecer al mismo grupo de recursos SQL.
- Asegúrese de que solo hay un iniciador VFC o FC conectado a cada host. Esto se debe a que, SnapCenter solo admite un iniciador por host.
- Si la base de datos de origen o la instancia de destino se encuentran en un volumen compartido de clúster (csv), la base de datos clonada se realizará en csv.

Para los entornos virtuales (VMDK/RDM), asegúrese de que el punto de montaje es un disco dedicado.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **complemento SnapCenter para SQL Server** en la lista.
  2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.

     No se admite la clonado del backup de una instancia.

- Pasos*
  1. Seleccione la base de datos o el grupo de recursos.
  2. En la página de visualización de **Manage Copies**, seleccione la copia de seguridad del sistema de almacenamiento principal o secundario (reflejado o en almacén).
  3. Seleccione el backup y, a continuación, haga clic en .
  4. En la página **Opciones de clonación**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Clone el servidor | Elija el host donde se debe crear el clon. |
| Instancia de clon | Seleccione la instancia de clonado en la que desea que se clone el backup de base de datos.<br><br>Esta instancia de SQL debe estar ubicada en el servidor de clones especificado. |
| Sufijo de clon | Introduzca el sufijo que se incorporará al nombre de archivo del clon para identificar que la base de datos es un clon.<br><br>Por ejemplo, *db1_clone*. Si clona en la misma ubicación que la de la base de datos original, debe proporcionar un sufijo para diferenciar la base de datos clonada de la original. De lo contrario, la operación dará error. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Auto assign Mount point o Auto assign volume Mount point under path | Elija si asignar automáticamente un punto de montaje o un punto de montaje de volumen en una ruta.<br><br>Auto assign volume Mount point under path: El punto de montaje en una ruta permite proporcionar un directorio específico. Los puntos de montaje se crearán dentro de ese directorio. Antes de seleccionar esta opción, debe asegurarse de que el directorio esté vacío. Si hay una base de datos en ese directorio, la base de datos presentará un estado no válido después de la operación de montaje. |

5. En la página **Logs**, seleccione una de las siguientes opciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Ninguno | Seleccione esta opción si solo desea clonar el backup completo sin ningún registro. |
| Todos los backups de registros | Seleccione esta opción para clonar todos los backups de registro disponibles con fecha posterior al backup completo. |
| Mediante backups de registros hasta que | Seleccione esta opción para clonar la base de datos según los registros de backup que se crearon hasta el registro de backup con la fecha seleccionada. |
| Por fecha específica hasta | Indique la fecha y la hora después de las cuales los registros de transacciones no se aplican a la base de datos clonada.<br><br>Esta clonado de momento específico detiene la clonado de las entradas del registro de transacciones que se registraron después de la fecha y la hora especificadas. |

6. En la página **Script**, introduzca el tiempo de espera de script, la ruta y los argumentos del script previo o posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente.

   Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

   El tiempo de espera predeterminado del script es 60 segundos.

7. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de clonado realizada, seleccione **Adjuntar informe de trabajo**.

Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

Para EMS, consulte "Gestione la recogida de datos de EMS"

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.
2. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Después de terminar**

Después de crear el clon, no debe cambiar nunca el nombre.

**Más información**

"Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad"

"Clonar backups mediante cmdlets de PowerShell"

"Es posible que la operación de clonado produzca errores o tarde más tiempo en finalizar con el valor TCP_TIMEOUT predeterminado"

"Se produce un error en el clon de la base de datos de la instancia de clúster"

## Ejecute el ciclo de vida del clon

Mediante SnapCenter, puede crear clones a partir de un grupo de recursos o una base de datos. Puede realizar un clon bajo demanda o programar operaciones de clonado periódicas de un grupo de recursos o una base de datos. Si clona un backup periódicamente, puede utilizar el clon para desarrollar aplicaciones, completar datos o recuperar datos.

SnapCenter permite programar varias operaciones de clonado para que se ejecuten simultáneamente ente varios servidores.

**Lo que necesitará**

- Mientras se clona en una instancia de base de datos independiente, asegúrese de que exista la ruta de acceso del punto de montaje y sea un disco dedicado.
- Al realizar la clonación en una instancia de clúster de conmutación por error (FCI, Failover Cluster Instance), asegúrese de que los puntos de montaje existen, son un disco compartido y la ruta de acceso y el FCI deben pertenecer al mismo grupo de recursos SQL.
- Si la base de datos de origen o la instancia de destino se encuentran en un volumen compartido de clúster (csv), la base de datos clonada se realizará en csv.

Para los entornos virtuales (VMDK/RDM), asegúrese de que el punto de montaje es un disco dedicado.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione **base de datos** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione el grupo de recursos o la base de datos y, a continuación, haga clic en **Clone Lifecycle**.
4. En la página **Opciones**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Nombre del trabajo de clonado | Especifique el nombre de trabajo de ciclo de vida de clon que ayuda en la supervisión y la modificación del trabajo de ciclo de vida de clon. |
| Clone el servidor | Elija el host en el que debe colocarse el clon. |
| Instancia de clon | Elija la instancia de clon en la que desea clonar la base de datos. Esta instancia de SQL debe estar ubicada en el servidor de clones especificado. |
| Sufijo de clon | Introduzca el sufijo que se incorporará a la base de datos de clones para identificar que se trata de un clon. Cada instancia de SQL que se utiliza para crear un grupo de recursos de clon debe tener un nombre de base de datos único. Por ejemplo, si el grupo de recursos del clon contiene una base de datos de origen «nb1» de una instancia de SQL «'inst1'» y «db1» se clona en «'inst1'», el nombre de la base de datos del clon deberá ser «db1*clone*». '"clone'" es un sufijo obligatorio definido por el usuario porque la base de datos se clona en la misma instancia. Si se clona «db1» en la instancia de SQL «'inst2'», el nombre de la base de datos clonada puede permanecer «db1» (el sufijo es opcional) porque la base de datos se clona en una instancia diferente. |
| Auto assign Mount point o Auto assign volume Mount point under path | Elija si asignar automáticamente un punto de montaje o un punto de montaje de volumen en una ruta. Si opta por asignar automáticamente un punto de montaje de volumen en una ruta, puede proporcionar un directorio específico. Los puntos de montaje se crearán dentro de ese directorio. Antes de seleccionar esta opción, debe asegurarse de que el directorio esté vacío. Si hay una base de datos en ese directorio, la base de datos presentará un estado no válido después de la operación de montaje. |

5. En la página **ubicación**, seleccione una ubicación de almacenamiento para crear un clon.
6. En la página **Script**, introduzca la ruta de acceso y los argumentos del script previo o posterior que se deben ejecutar antes o después de la operación de clonado, según corresponda.

   Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

   El tiempo de espera predeterminado del script es 60 segundos.

7. En la página **Programación**, realice una de las siguientes acciones:
   - Seleccione **Ejecutar ahora** si desea ejecutar el trabajo de clonado inmediatamente.
   - Seleccione **Configure schedule** cuando desea determinar la frecuencia con la que debe producirse la operación de clonado, cuándo debe iniciarse la programación de clonado, en qué día debe producirse la programación de clonado, cuándo debe caducar la programación y si los clones tienen que eliminarse cuando caduque la programación.
8. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de clonado realizada, seleccione **Adjuntar informe de trabajo**.

   Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

Para EMS, consulte "Gestione la recogida de datos de EMS"

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Debe supervisar el proceso de clonación mediante la página **Monitor** > **Jobs**.

## Supervisar operaciones de clonado de bases de datos de SQL

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

**Acerca de esta tarea**

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Clonar**.
   d. En la lista desplegable **Estado**, seleccione el estado del clon.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Cancelar las operaciones de clonado de recursos SQL

Es posible cancelar las operaciones de clonado que se encuentran en cola.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de clonado.

**Acerca de esta tarea**

- Es posible cancelar una operación de clonado en cola desde la página Monitor o el panel Activity.
- No se puede cancelar una operación de clonado en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de clonado en cola.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de clonación en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione la operación y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar la operación de clonado, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

# Proteger las bases de datos SAP HANA

## Plugin de SnapCenter para base de datos SAP HANA

### Información general sobre el plugin de SnapCenter para bases de datos de SAP HANA

El plugin de SnapCenter para bases de datos de SAP HANA es un componente del lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de bases de datos de SAP HANA. El plugin para bases de datos de SAP HANA automatiza el backup, la restauración y la clonado de bases de datos de SAP HANA en el entorno de SnapCenter.

SnapCenter admite contenedores individuales y contenedores de bases de datos multitenant (MDC). Es posible utilizar el plugin para base de datos SAP HANA tanto en entornos de Windows como de Linux. El plugin que no está instalado en el host de la base de datos HANA se conoce como plugin de host centralizado. El complemento de host centralizado puede gestionar varias bases de datos HANA en diferentes hosts.

Cuando se instala el plugin para bases de datos de SAP HANA, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear copias de reflejo de conjuntos de backups en otro volumen. También es posible utilizar el plugin con la tecnología SnapVault de NetApp para realizar replicaciones de backup disco a disco para cumplimiento de normativas.

### Tareas que pueden llevarse a cabo con el plugin de SnapCenter para base de datos SAP HANA

Cuando el plugin para base de datos SAP HANA está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar bases de datos SAP HANA y sus recursos. También es posible ejecutar tareas complementarias a estas operaciones.

- Agregar bases de datos.
- Crear backups.
- Restaurar desde backups.
- Clonar backups.
- Programar operaciones de backup.
- Supervisar operaciones de backup, de restauración y de clonado.
- Ver informes para operaciones de backup, restauración y clonado.

### Funciones del plugin de SnapCenter para base de datos SAP HANA

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para bases de datos de SAP HANA, se utiliza la interfaz gráfica de usuario de SnapCenter.

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar operaciones de backup, restauración y clonado consistentes entre plugins, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins.

- **Administración central automatizada**

  Es posible programar operaciones de backup, configurar la retención de backup basado en políticas y realizar operaciones de restauración. También es posible supervisar de manera proactiva el entorno configurando SnapCenter para que envíe alertas por correo electrónico.

- **Tecnología de copia snapshot de NetApp** no disruptiva

  SnapCenter utiliza la tecnología de copias de Snapshot de NetApp con el plugin para bases de datos de SAP HANA para realizar backups de recursos.

Usar el plugin para bases de datos de SAP HANA también ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración y clonado
- Seguridad compatible con RBAC y delegación de roles centralizada

  También es posible configurar las credenciales para que los usuarios de SnapCenter autorizados tengan permisos en el nivel de las aplicaciones.

- Creación de copias de recursos con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

  Se requiere una licencia de FlexClone en el sistema de almacenamiento donde desea crear el clon.

- Compatibilidad con la función de copia de Snapshot de grupo de consistencia de ONTAP como parte de la creación de backups.
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de recursos

  En una sola operación se consolidan copias de Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear copias de Snapshot con comandos externos.
- Compatibilidad con backups basados en archivos.
- Compatibilidad con LVM de Linux en el sistema de archivos XFS.

## Tipos de almacenamiento compatibles con el plugin de SnapCenter para base de datos SAP HANA

SnapCenter es compatible con una amplia gama de tipos de almacenamiento tanto en máquinas físicas como máquinas virtuales (VM). Debe verificar la compatibilidad de su tipo de almacenamiento antes de instalar el plugin de SnapCenter para base de datos SAP HANA.

| Máquina | Tipo de almacenamiento |
| --- | --- |
| Servidores físicos y virtuales | LUN conectados a FC |

| Máquina | Tipo de almacenamiento |
| --- | --- |
| Servidor físico | LUN conectados a iSCSI |
| Servidores físicos y virtuales | Volúmenes conectados en NFS |

## Privilegios mínimos requeridos de ONTAP

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

| **Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores** |
| --- |
| event generate-autosupport-log |
| se muestra el historial del trabajo<br><br>detención de trabajo |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| lun |
| lun create |
| eliminación de lun |
| igroup de lun añadido |
| crear lun igroup |
| lun igroup eliminado |
| cambio de nombre de lun igroup |
| lun igroup show |
| asignación de lun de nodos adicionales |
| se crea la asignación de lun |
| se elimina la asignación de lun |
| asignación de lun quitar nodos de generación de informes |
| se muestra el mapa de lun |
| modificación de lun |
| movimiento de lun en volumen |
| lun desconectada |
| lun conectada |
| reserva persistente de lun clara |
| cambio de tamaño de lun |
| serie de lun |
| muestra de lun |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| regla adicional de la política de snapmirror<br>regla de modificación de la política de snapmirror<br>regla de eliminación de la política de snapmirror<br>la política de snapmirror<br>restauración de snapmirror<br>de snapmirror<br>historial de snapmirror<br>actualización de snapmirror<br>conjunto de actualizaciones de snapmirror<br>destinos de listas de snapmirror |
| versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| crear el clon de volumen |
| show de clon de volumen |
| inicio de división de clon de volumen |
| detención de división de clon de volumen |
| cree el volumen |
| destrucción del volumen |
| crear el archivo de volumen |
| uso show-disk del archivo de volumen |
| volumen sin conexión |
| volumen en línea |
| modificación del volumen |
| crear el qtree de volúmenes |
| eliminación de qtree de volumen |
| modificación del qtree del volumen |
| se muestra volume qtree |
| restricción de volumen |
| visualización de volumen |
| crear snapshots de volumen |
| eliminación de snapshots de volumen |
| modificación de las copias de snapshot de volumen |
| cambio de nombre de copias de snapshot de volumen |
| restauración de copias snapshot de volumen |
| archivo de restauración de snapshots de volumen |
| visualización de copias de snapshot de volumen |
| desmonte el volumen |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| vserver cifs |
| vserver cifs share create |
| eliminación de vserver cifs share |
| se muestra vserver shadowcopy |
| visualización de vserver cifs share |
| visualización de vserver cifs |
| política de exportación de vserver |
| creación de política de exportación de vserver |
| eliminación de la política de exportación de vserver |
| creación de reglas de política de exportación de vserver |
| aparece la regla de política de exportación de vserver |
| visualización de la política de exportación de vserver |
| vserver iscsi |
| se muestra la conexión iscsi del vserver |
| se muestra vserver |

| Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| interfaz de red |
| se muestra la interfaz de red |
| vserver |

## Preparar los sistemas de almacenamiento para la replicación SnapMirror y SnapVault para las bases de datos SAP HANA

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en

el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

## Estrategia de backup para las bases de datos SAP HANA

### Defina una estrategia de backup para las bases de datos SAP HANA

Definir una estrategia de backup antes de crear las tareas de backup ayuda a garantizar que se cuente con todos los backups necesarios para restaurar o clonar correctamente los recursos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

#### Acerca de esta tarea

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

- Pasos*
  1. Determinar cuándo se debe realizar el backup de los recursos.
  2. Decidir cuántas tareas de backup se necesitan.
  3. Decidir el nombre que se asignará a los backups.
  4. Decidir si se desea crear una política basada en copias de Snapshot para realizar backup de las copias de Snapshot consistentes con las aplicaciones de la base de datos.
  5. Decidir si se verificará la integridad de la base de datos.
  6. Decidir si se desean usar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
  7. Determinar el período de retención para las copias de Snapshot en el sistema de almacenamiento de origen y el destino de SnapMirror.
  8. Determinar si se desean ejecutar comandos antes o después de la operación de backup y proporcionar un script previo o posterior.

### Detección automática de recursos en el host Linux

Los recursos son bases de datos de SAP HANA y volumen de datos no data en el host Linux que gestiona SnapCenter. Después de instalar el plugin de SnapCenter para el plugin de base de datos SAP HANA, las bases de datos SAP HANA en ese host Linux se detectan automáticamente y se muestran en la página Resources.

La detección automática es compatible con los siguientes recursos de SAP HANA:

- Contenedores individuales

  Después de instalar o actualizar el plugin, los recursos de contenedor único ubicados en un plugin de host centralizado continuarán siendo recursos añadidos manualmente.

  Después de instalar o actualizar el plugin, las bases de datos SAP HANA se detectan de forma automática solo en los hosts SAP HANA Linux, que se registran directamente en SnapCenter.

- Contenedor de base de datos multitenant (MDC)

  Después de instalar o actualizar el plugin, los recursos de MDC ubicados en un plugin de host centralizado continuarán siendo un recurso añadido manualmente.

  Debe continuar añadiendo manualmente los recursos del MDC en el plugin del host centralizado después de actualizar a SnapCenter 4.3.

  Para los hosts SAP HANA Linux registrados directamente en SnapCenter, instalar o actualizar el plugin provocará una detección automática de los recursos del host. Después de actualizar el plugin, para cada recurso MDC ubicado en el host del plugin, se descubre automáticamente otro recurso MDC con un formato GUID diferente y se registra en SnapCenter. El nuevo recurso estará bloqueado.

  Por ejemplo, en SnapCenter 4.2, si el recurso de E90 MDC se encuentra en el host del plugin y se registró manualmente, después de actualizar a SnapCenter 4.3, se detecta otro recurso de E90 MDC con un GUID diferente y se registra en SnapCenter.

La guía de protección de datos para bases de datos de SAP HANA tiene más información sobre cómo trabajar con el nuevo recurso MDC en un host de plugins de SnapCenter para operaciones de protección de datos

La detección automática no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

  Si se detectan los recursos anteriores, las operaciones de protección de datos no son compatibles con estos recursos.

- Configuración de varios hosts DE HANA
- Replicación de sistemas HANA
- Varias instancias en el mismo host

**Tipo de backups admitido**

## El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite los tipos de backups basados en archivos y backups basados en copias de Snapshot para bases de datos de SAP HANA.

#### Backups basados en archivos

Los backups basados en archivos verifican la integridad de la base de datos. Es posible programar una operación de backup basado en archivos para que se produzca en intervalos específicos. Solo se realiza un backup de los inquilinos activos. No es posible restaurar ni clonar backups basados en archivos desde SnapCenter.

#### Backup basado en copia de Snapshot

Los backups basados en copia de Snapshot aprovechan la tecnología de copia de Snapshot de NetApp para crear copias en línea y de solo lectura de los volúmenes en los cuales residen las bases de datos de SAP HANA.

#### Cómo usa el plugin de SnapCenter para base de datos SAP HANA las copias de Snapshot de grupos de consistencia

Es posible usar el plugin para crear copias Snapshot de grupos de consistencia para los grupos de recursos. Un grupo de consistencia es un contenedor que puede albergar varios volúmenes para que se gestionen como una misma entidad. Un grupo de consistencia es un conjunto de copias de Snapshot simultáneas de varios volúmenes, que ofrece copias consistentes de un grupo de volúmenes.

También es posible especificar un tiempo de espera para la controladora de almacenamiento a fin de agrupar de forma coherente las copias de Snapshot. Las opciones de tiempo de espera disponibles son **Urgent**, **Medium** y **Relaxed**. También es posible habilitar o deshabilitar la sincronización de Write Anywhere File Layout (WAFL) durante la operación de copia de Snapshot de grupos consistentes. La sincronización WAFL mejora el rendimiento de una copia de Snapshot de grupo de consistencia.

#### Cómo hace SnapCenter para gestionar el mantenimiento de backups de registros y datos

SnapCenter gestiona el mantenimiento de los backups de registros y de datos en los niveles de sistema de almacenamiento y sistema de archivos, y dentro del catálogo de backup SAP HANA.

Las copias de Snapshot en el almacenamiento primario y secundario y sus entradas correspondientes en el catálogo SAP HANA se eliminan de acuerdo con la configuración de retención. Las entradas del catálogo SAP HANA también se eliminan durante la eliminación de grupos de backup y recursos.

#### Consideraciones para determinar programaciones de backup para base de datos SAP HANA

El factor más importante para determinar una programación de backup es la tasa de cambio del recurso. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores que se deben tener en cuenta son la importancia del recurso para la organización, el SLA y el RPO.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup (cada cuánto se realizan los backups)

  La frecuencia de backup, también denominada tipo de programación para algunos plugins, es parte de una configuración de políticas. Por ejemplo, se puede configurar una frecuencia de backup horaria, diaria, semanal o mensual.

- Programaciones de backup (exactamente cuándo se realizan los backups)

  Las programaciones de backup forman parte de la configuración de un recurso o un grupo de recursos. Por ejemplo, si hay un grupo de recursos con una política configurada para realizar un backup semanal, es posible configurar la programación para que se realice un backup todos los jueves a las 00:10

#### Cantidad de tareas de backup necesarias para bases de datos SAP HANA

Algunos factores que determinan la cantidad de trabajos de backup que se necesitan son el tamaño del recurso, la cantidad de volúmenes que se usan, la tasa de cambio del recurso y el acuerdo de nivel de servicio.

#### Convenciones de nomenclatura de backups para bases de datos del plugin para SAP HANA

Es posible usar la convención de nomenclatura de copia Snapshot predeterminada o usar una convención de nomenclatura personalizada. La convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de las copias de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La copia Snapshot usa la siguiente convención de nomenclatura predeterminada:

```
resourcegroupname_hostname_timestamp
```

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre de host.
- *03-12-2015_23.17.26* es la fecha y la marca de hora.

Como alternativa, puede especificar el formato de nombre de la copia Snapshot mientras protege los recursos o grupos de recursos seleccionando **usar formato de nombre personalizado para copia Snapshot**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la copia de Snapshot.

## Estrategia de restauración y recuperación para bases de datos SAP HANA

#### Defina una estrategia de restauración y recuperación para recursos de SAP HANA

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar una base de datos.

- Pasos*
  1. Determinar las estrategias de restauración compatibles con los recursos SAP HANA añadidos manualmente
  2. Determinar las estrategias de restauración compatibles con las bases de datos SAP HANA detectadas automáticamente
  3. Decidir el tipo de operaciones de recuperación que se desea ejecutar.

### Tipos de estrategias de restauración compatibles con los recursos de SAP HANA añadidos manualmente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter. Existen dos tipos de estrategias de restauración para los recursos de SAP HANA que se añaden manualmente. No puede recuperar los recursos de SAP HANA añadidos manualmente.

No puede recuperar los recursos de SAP HANA añadidos manualmente.

#### Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

#### Restauración de nivel de archivos

- Restaura los archivos de volúmenes, qtrees o directorios
- Restaura solo los LUN seleccionados

### Tipos de estrategias de restauración compatibles para las bases de datos SAP HANA detectadas automáticamente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter. Existen dos tipos de estrategias de restauración para las bases de datos SAP HANA detectadas automáticamente.

#### Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso
  - Debe seleccionarse la opción **revertir volumen** para restaurar todo el volumen.

Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

#### Base de datos de tenant

- Restaura la base de datos de tenant

Si se selecciona la opción **base de datos de inquilino**, deben utilizarse secuencias de comandos de recuperación de HANA Studio o HANA externas a SnapCenter para realizar la operación de recuperación.

### Tipos de operaciones de restauración para las bases de datos SAP HANA detectadas automáticamente

SnapCenter admite tipos de restauración SnapRestore (VBSR) basada en volúmenes, SnapRestore de archivos individuales y restauración por conexión y copia para bases de datos SAP HANA detectadas automáticamente.

**La SnapRestore basada en volúmenes (VBSR) se realiza en entornos NFS para las siguientes situaciones:**

- Cuando la copia de seguridad seleccionada para restaurar se realiza en versiones anteriores a SnapCenter 4.3 y sólo si se selecciona la opción **Complete Resource**
- Cuando la copia de seguridad seleccionada para restaurar se realiza en SnapCenter 4.3, y si la opción **revertir volumen** está seleccionada

**Single File SnapRestore se realiza en entornos NFS en los siguientes casos:**

- Cuando la copia de seguridad seleccionada para restaurar se realiza en SnapCenter 4.3, y si sólo se selecciona la opción **completar recurso**
- Para contenedores de bases de datos multitenant (MDC), cuando la copia de seguridad seleccionada para restaurar se realiza en SnapCenter 4.3 y se selecciona la opción **base de datos de tenant**
- Cuando la copia de seguridad seleccionada se realiza desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **completar recurso**

**Single File SnapRestore se realiza en entornos SAN en los siguientes casos:**

- Cuando se realizan copias de seguridad en versiones anteriores a SnapCenter 4.3, y sólo si se selecciona la opción **recurso completo**
- Cuando se realizan copias de seguridad en SnapCenter 4.3 y sólo si se selecciona la opción **recurso completo**
- Cuando se selecciona la copia de seguridad de una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Complete Resource**

**La restauración basada en la conexión y la copia se realiza en entornos SAN para el siguiente escenario:**

- Para MDC, cuando la copia de seguridad seleccionada para restore se realiza en SnapCenter 4.3 y se selecciona la opción **base de datos de inquilinos**

Las opciones **Complete Resource**, **Volume Revert** y **Tenant Database** están disponibles en la página Restore Scope.

### Tipos de operaciones de recuperación compatibles con las bases de datos SAP HANA

SnapCenter le permite realizar diferentes tipos de operaciones de recuperación para las bases de datos SAP HANA.

- Recupere la base de datos hasta el estado más reciente
- Recupere la base de datos hasta un momento específico

  Debe especificar la fecha y la hora de la recuperación.

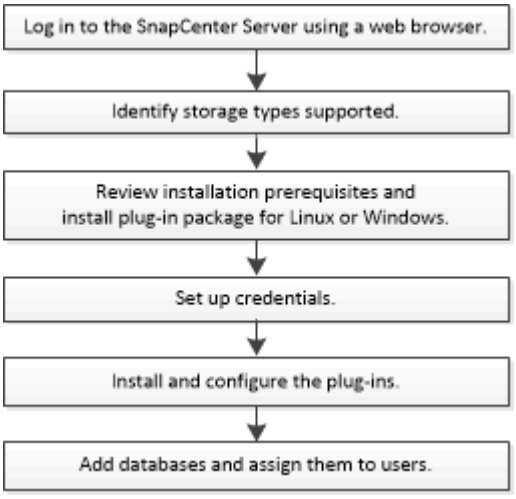
- Recuperar la base de datos hasta un backup de datos específico

SnapCenter también proporciona la opción no recovery para las bases de datos SAP HANA.

# Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA

## Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA

Debe instalar y configurar el plugin de SnapCenter para base de datos SAP HANA si desea proteger las bases de datos SAP HANA.




## Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. Plugin SnapCenter para base de datos SAP HANA está disponible en entornos Windows y Linux.

- Debe haber instalado Java 1.8 64 bit en su host.

  IBM Java no es compatible.

- Debe haber instalado el terminal interactivo de base de datos SAP HANA (cliente HDBSQL) en el host.
- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows "'LocalSystem'", que es el comportamiento predeterminado cuando el plugin para base de datos SAP HANA se instala como administrador de dominio.
- Para Windows, se deben crear claves de almacenamiento como usuario SYSTEM.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host. El plugin de SnapCenter para Microsoft Windows se pondrá en marcha de forma predeterminada con el plugin de SAP HANA en hosts Windows.
- Para host Linux, se accede a las claves de almacenamiento de usuario seguro HDB como usuario de sistema operativo HDBSQL.

- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host de base de datos SAP HANA.

**Host Windows**

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Cuando se instala el plugin para base de datos SAP HANA en un host Windows, el plugin de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 1.8 64 bit en su host de Windows.

  "Descargas de Java para todos los sistemas operativos"

  La "Herramienta de matriz de interoperabilidad" contiene la información más reciente acerca de los requisitos.

**Hosts Linux**

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 1.8 64 bit en su host Linux.

  "Descargas de Java para todos los sistemas operativos"

  La "Herramienta de matriz de interoperabilidad" contiene la información más reciente acerca de los requisitos.

- Para bases de datos SAP HANA que se ejecutan en un host Linux, mientras se instala el plugin para base de datos SAP HANA, el plugin de SnapCenter para UNIX se instala automáticamente.

## Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux

Antes de instalar el paquete de plugins de SnapCenter para Linux, tiene que conocer bien algunos requisitos básicos de espacio y tamaño del sistema host.

| Elemento | Requisitos |
|---|---|
| Sistemas operativos | • Red Hat Enterprise Linux<br>• SUSE Linux Enterprise Server (SLES)<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |

| Elemento | Requisitos |
| --- | --- |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 2 GB<br><br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía, según la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |
| Paquetes de software obligatorios | Tipos Java 1.8.x (64 bits)Oracle Java y OpenJDK<br><br>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". . |

## Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar los plugins de SnapCenter, y credenciales adicionales para realizar operaciones de protección de datos en sistemas de archivos Windows o bases de datos.

### Acerca de esta tarea

- Hosts Linux

  Debe configurar credenciales para instalar plugins en hosts Linux.

  Debe configurar las credenciales para el usuario raíz o un usuario que no sea raíz que tenga privilegios sudo para instalar e iniciar el proceso del plugin.

  **Práctica recomendada:** aunque se permite crear credenciales para Linux después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

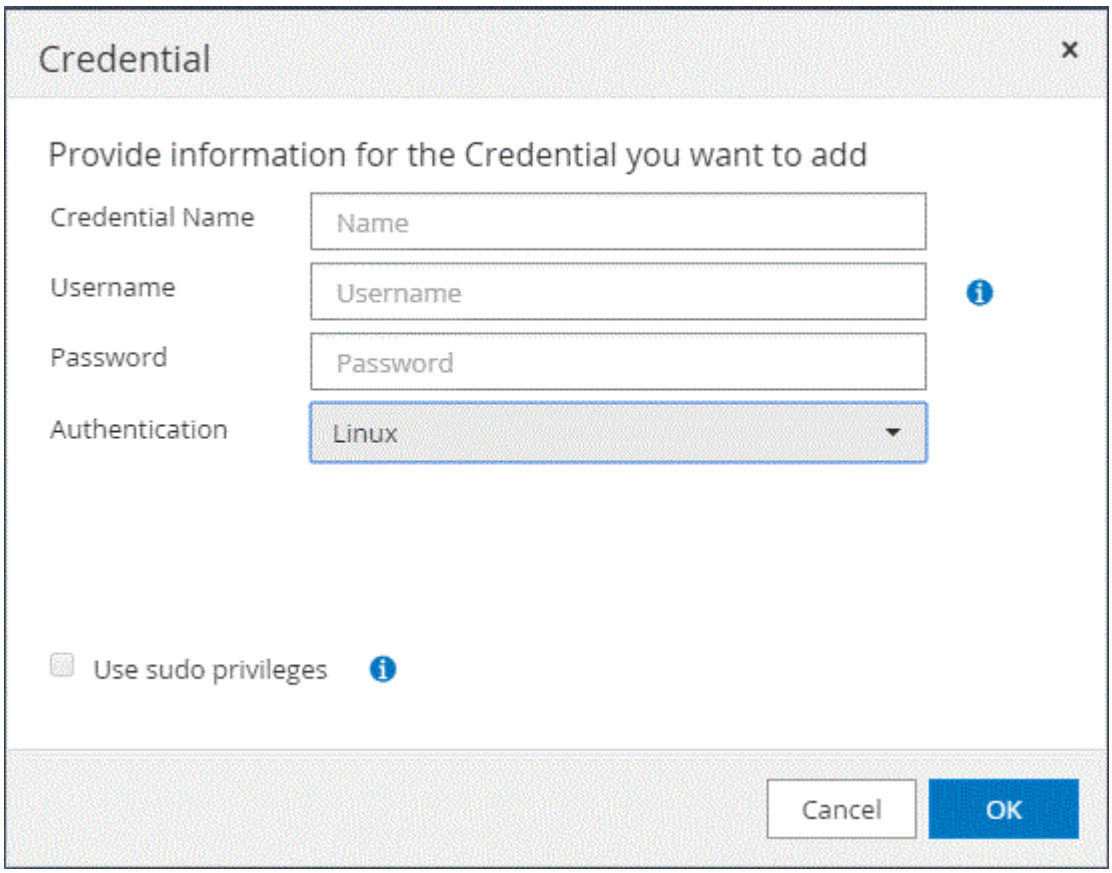
- Host Windows

Debe configurar credenciales de Windows antes de instalar plugins.

Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.

Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al nombre de usuario.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página **Configuración**, haga clic en **credenciales**.
  3. Haga clic en **Nuevo**.




  4. En la página **Credential**, especifique la información necesaria para configurar las credenciales:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de credencial | Introduzca un nombre para las credenciales. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario | Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.<br>• Administrador de dominio o cualquier miembro del grupo de administradores<br>Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:<br>◦ *NetBIOS\Username*<br>◦ *Domain FQDN\Username*<br>• Administrador local (sólo para grupos de trabajo)<br>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: *Username*<br>No utilice comillas dobles (") ni marcas de retroceso (') en las contraseñas. No debe usar el signo menos de (<) y el signo de exclamación (!) los símbolos juntos en las contraseñas. Por ejemplo, arrendhan<!10, les10<!, backtick'12. |
| Contraseña | Introduzca la contraseña usada para autenticación. |
| Modo de autenticación | Seleccione el modo de autenticación que desea utilizar. |
| Use privilegios sudo | Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz.<br>Aplicable únicamente a usuarios Linux. |

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede que desee asignar mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

## Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

**Lo que necesitará**

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

   1. Asigne los privilegios administrativos al GMSA configurado en el host.
   2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

      El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

## Instale el plugin de SnapCenter para base de datos SAP HANA

### Añada hosts e instale paquetes de plugins en hosts remotos

Debe usar la página SnapCenter Add Host para añadir hosts y, a continuación, instalar los paquetes de los plugins. Los plugins se instalan automáticamente en hosts remotos. Puede añadir un host e instalar paquetes de plugins para un host individual o para un clúster.

#### Lo que necesitará

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Debe asegurarse de que el servicio de cola de mensajes está en ejecución.
- La documentación de administración contiene información sobre la gestión de los hosts.

- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configure la cuenta de servicio gestionado de grupo en Windows Server 2012 o posterior para SAP HANA"

**Acerca de esta tarea**

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
  3. Haga clic en **Agregar**.
  4. En la página **hosts**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de host | Seleccione el tipo de host:<br>• Windows<br>• Linux<br>El plugin para SAP HANA está instalado en el host de cliente de HDBSQL, y este host puede estar en un sistema Windows o Linux. |
| Nombre de host | Introduzca el nombre de host de comunicación. Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.<br>Debe configurar al cliente de HDBSQL y a HDBUserStore en este host. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Credenciales | Seleccione el nombre de credencial que ha creado o cree nuevas credenciales. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales.<br><br>Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado.<br><br>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. |

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. |
| Ruta de instalación | El plugin para SAP HANA está instalado en el host de cliente de HDBSQL, y este host puede estar en un sistema Windows o Linux.<br><br>• En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta.<br>• Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Omitir comprobaciones previas a la instalación | Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin. |
| Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in | En el caso de host de Windows, seleccione esta casilla de comprobación si desea utilizar una cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de plugin.<br>Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName $.<br>GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows. |

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

   Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en C:\Program Files\NetApp\SnapCenter WebApp para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero debe solucionar el problema.

   En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Si el tipo de host es Linux, verifique la huella digital y, a continuación, haga clic en **Confirmar y enviar**.

   En una configuración de clúster, debe comprobar la huella de cada uno de los nodos del clúster.

   La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

1. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación están en /custom_location/snapcenter/logs.

### Instale paquetes de plugins de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de plugins de SnapCenter para Linux o Windows en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

#### Lo que necesitará

Debe haberse registrado en SnapCenter como usuario del dominio con derechos de administrador local en cada host en el que desee instalar el paquete de plugins.

- Pasos*

  1. Inicie PowerShell.
  2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
  3. Instale el plugin en varios hosts mediante el cmdlet Install-SmHostPackage y los parámetros requeridos.

     La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

  Puede utilizar la opción -skipprecheck cuando haya instalado los plugins manualmente y no quiera validar si el host cumple los requisitos para instalar el plugin.

  1. Introduzca sus credenciales para la instalación remota.

### Instale el plugin de SnapCenter para base de datos SAP HANA en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para base de datos SAP HANA mediante la interfaz de usuario de SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar el plugin para base de datos SAP HANA en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

#### Lo que necesitará

- Debe instalar el plugin para base de datos SAP HANA en cada host Linux en el que resida el cliente HDBSQL.
- El host Linux en el que se instala el plugin de SnapCenter para base de datos SAP HANA debe cumplir con los requisitos dependientes de software, base de datos y sistema operativo.

  La herramienta de matriz de interoperabilidad (IMT) contiene la última información sobre las configuraciones soportadas.

  "Herramienta de matriz de interoperabilidad de NetApp"

- El plugin de SnapCenter para base de datos SAP HANA forma parte del paquete de plugins de SnapCenter para Linux. Antes de instalar el paquete de plugins de SnapCenter para Linux, debe haber instalado SnapCenter en un host de Windows.

- Pasos*

1. Copie el paquete de plugins de SnapCenter para el archivo de instalación de Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar el plugin para la base de datos SAP HANA.

   Puede acceder a esta ruta desde el host en el que está instalado el servidor SnapCenter.

2. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el archivo de instalación.
3. Instale el plugin: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
   - -DPORT indica el puerto de comunicación HTTPS de SMCore.
   - -DSERVER_IP indica la dirección IP del servidor SnapCenter.
   - -DSERVER_HTTPS_PORT indica el puerto HTTPS del servidor SnapCenter.
   - -DUSER_INSTALL_DIR indica el directorio en el que desea instalar el paquete de plugins de SnapCenter para Linux.
   - DINSTALL_LOG_NAME indica el nombre del archivo de registro.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

1. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y añada el parámetro PLUGINS_ENABLED = hana:3.0.
2. Añada el host al servidor de SnapCenter con el cmdlet Add-Smhost y los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

### Supervise el estado de la instalación del plugin para SAP HANA

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error

- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de instalación.
     e. Haga clic en **aplicar**.
  4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configurar certificado de CA

### Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

> Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

### Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

- Pasos*
  1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
  2. En la ventana **Agregar o quitar complementos**, seleccione **certificados** y, a continuación, haga clic en **Agregar**.

3. En la ventana del complemento **certificados**, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
|---|---|
| Importar clave privada | Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**. |
| Importar formato de archivo | No realice cambios; haga clic en **Siguiente**. |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |
| Finalización del Asistente para importación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación. |

> El certificado de importación debe incluirse con la clave privada (los formatos admitidos son: *.pfx, *.p12, *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

**Obtenga la huella digital del certificado de CA**

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

- Pasos*
  1. Realice lo siguiente en la interfaz gráfica de usuario:
     a. Haga doble clic en el certificado.
     b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
     c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
     d. Copie los caracteres hexadecimales del cuadro.
     e. Quite los espacios entre los números hexadecimales.

        Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

  2. Realice lo siguiente desde PowerShell:
     a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

*Get-ChildItem -Path Cert:\LocalMachine\My*

b. Copie la huella digital.

**Configure el certificado de CA con servicios de plugins de host de Windows**

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

- Pasos*

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

   Por ejemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Enlace el certificado recientemente instalado con los servicios de
   plugins del host de Windows mediante la ejecución de los siguientes
   comandos:
   ```

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid"
   ```

   Por ejemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

**Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Linux**

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo 'keystore.jks', que se encuentra en

*/opt/NetApp/snapcenter/scc/etc* tanto como en su almacén de confianza como en su almacén de claves.

**Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso**

- Pasos*

1. Puede recuperar la contraseña predeterminada del almacén de claves del plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

   Es el valor correspondiente a la clave 'KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

3. Reinicie el servicio después de cambiar la contraseña.

> La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

**Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado**

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado: /Opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Añada un certificado raíz o intermedio:

   ```
    keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza del plugin personalizado.
   ```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

#### Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado /opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Agregue el certificado de CA con clave pública y privada.

   ```
   keytool -importkeystore -srckeystore
   /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore
   keystore.jks -deststoretype JKS
   ```

5. Enumere los certificados añadidos al almacén de claves.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Si el nombre del alias del certificado de CA es largo y contiene
   espacio o caracteres especiales ("*",","), cambie el nombre del alias
   por un nombre simple:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias
   "simple_alias" -keystore keystore.jks
   . Configure el nombre del alias del certificado de CA en el archivo
   agent.properties.
   ```

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

8. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

#### Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

### Acerca de esta tarea

- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es ' opt/NetApp/snapcenter/scc/etc/crl'.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

     Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

## Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Windows

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*, tanto como su almacén de confianza como su almacén de claves.

#### Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

- Pasos*

  1. Puede recuperar la contraseña predeterminada del almacén de claves del plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

     Es el valor que corresponde a la clave *KEYSTORE_PASS*.

  2. Cambie la contraseña del almacén de claves:

     *keytool -storepasswd -keystore.jks*

     > Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool por su ruta completa.

     *C:\Archivos de programa\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore.jks*

  3. Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves:

     *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

1. Reinicie el servicio después de cambiar la contraseña.

> La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

**Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado**

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
  2. Busque el archivo 'keystore.jks'.
  3. Enumere los certificados añadidos al almacén de claves:

     *keytool -list -v -keystore.jks*

  4. Añada un certificado raíz o intermedio:

     *Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks*

  5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza del plugin personalizado.

> Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

**Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado**

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
  2. Busque el archivo *keystore.jks*.
  3. Enumere los certificados añadidos al almacén de claves:

     *keytool -list -v -keystore.jks*

  4. Agregue el certificado de CA con clave pública y privada.

     *Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -deststoretype JKS*

  5. Enumere los certificados añadidos al almacén de claves.

     *keytool -list -v -keystore.jks*

  6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.

7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

*Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks*

1. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

2. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

#### Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

**Acerca de esta tarea**

- Para descargar el último archivo CRL del certificado de CA relacionado, consulte "Cómo actualizar el archivo de lista de revocación de certificados en el certificado de CA de SnapCenter".
- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es *'C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la CLAVE CRL_PATH.
  2. Puede colocar más de un archivo CRL en este directorio.

     Los certificados entrantes se verificarán en cada CRL.

### Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

**Lo que necesitará**

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.

4. Haga clic en **más opciones**.
5. Seleccione **Activar validación de certificados**.

**Después de terminar**

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

# Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

## Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

## Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

# Prepárese para la protección de datos

## Requisitos previos para usar el plugin de SnapCenter para base de datos SAP HANA

Antes de utilizar el plugin de SnapCenter para base de datos SAP HANA, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas de requisitos previos.

- Instalar y configurar SnapCenter Server.

- Inicie sesión en el servidor SnapCenter.
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento y creando credenciales, si es necesario.
- Instale Java 1.7 o Java 1.8 en su host Linux o Windows.

  Debe configurar la ruta de Java en la variable de rutas del entorno del equipo host.

- Configure SnapMirror y SnapVault si quiere realizar una replicación de backup.
- Instale el cliente HDBSQL en el host donde va a instalar el plugin para base de datos SAP HANA.

  Configure las claves de almacenamiento de usuario para los nodos SAP HANA que va a gestionar a través de este host.

- En el caso de la base de datos SAP HANA 2.0SPS05, si va a utilizar una cuenta de usuario de base de datos SAP HANA, asegúrese de tener los siguientes permisos para realizar operaciones de backup, restauración y clonado en SnapCenter Server:
  - Administrador de backups
  - Catálogo leído
  - Administrador de backup de bases de datos
  - Operador de recuperación de bases de datos

## Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger bases de datos SAP HANA

Antes de usar SnapCenter, es necesariol comprender ciertos conceptos básicos vinculados con las operaciones de backup, clonado y restauración que se ejecutan. El usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos normalmente son bases de datos SAP HANA que se clonan o se incluyen en un backup mediante SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupacion de recursos en un host.

  Al realizar una operación con un grupo de recursos, esta se ejecuta en los recursos definidos en el grupo de acuerdo con la programación que se especificó para dicho grupo de recursos.

  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

- Las políticas especifican la frecuencia de backup, la replicación, los scripts y otras características de las operaciones de protección de datos.

  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. Asimismo, puede seleccionar una política al realizar un backup bajo demanda para un recurso individual.

Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando crea el grupo de recursos y asocia las políticas, puede configurar el grupo de recursos para que lleve a cabo un backup

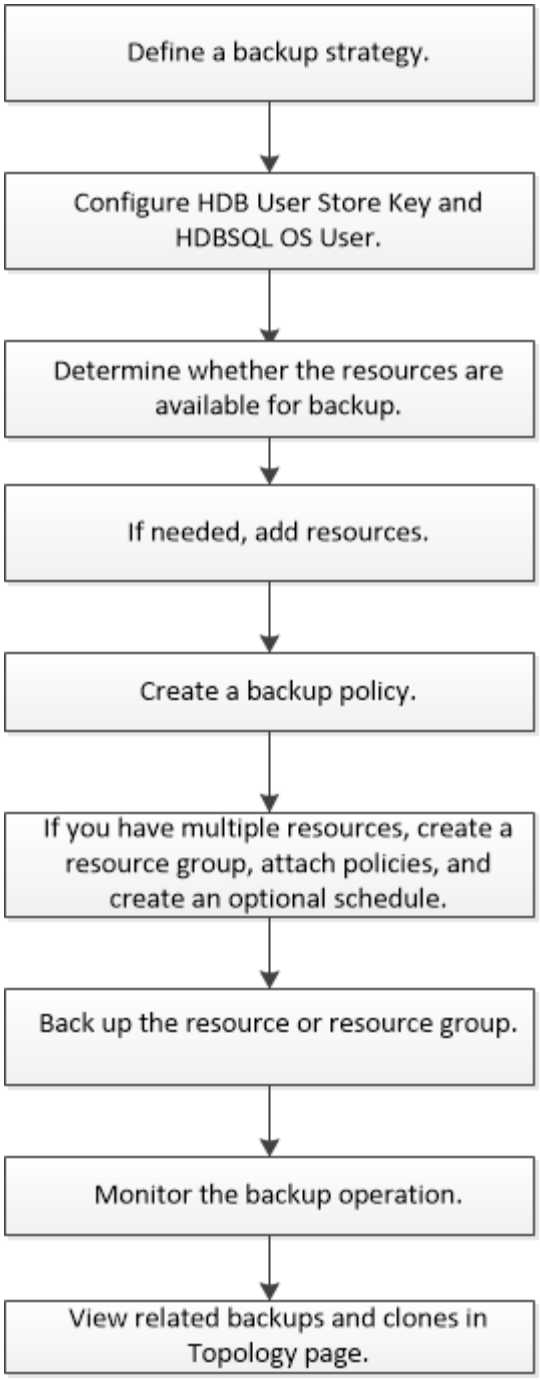
completo a diario.

# Realice un backup de los recursos de SAP HANA

## Realice un backup de los recursos de SAP HANA

Es posible crear un backup de un recurso (base de datos) o un grupo de recursos. El flujo de trabajo de backup incluye planificar, identificar las bases de datos para backup, gestionar las políticas de backup, crear grupos de recursos y adjuntar políticas, crear backups y supervisar las operaciones.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda sobre cmdlet de SnapCenter y la información de referencia sobre cmdlet contienen más información acerca de cmdlets de PowerShell.https://library.netapp.com/ecm/ecm_download_file/ECMLP2877143["Guía de referencia de cmdlets de SnapCenter Software"^].

## Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA

Debe configurar la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para realizar operaciones de protección de datos en bases de datos SAP HANA.

**Lo que necesitará**

- Si la base de datos SAP HANA no tiene la clave de almacenamiento de usuario seguro HDB y el usuario de sistema operativo SQL HDB configurados, aparece un icono de candado rojo solo para los recursos detectados automáticamente. Si durante una operación de detección posterior, se encontró que la clave de almacenamiento de usuario seguro HDB configurada era incorrecta o no proveía acceso a la base de datos, entonces el icono de candado rojo volverá a aparecer.
- Es necesario configurar la clave de almacenamiento de usuario seguro HDB y el usuario del sistema operativo HDB SQL para proteger la base de datos, o bien añadirla a un grupo de recursos para realizar operaciones de protección de datos.
- Debe configurar HDB SQL OS User para acceder a la base de datos del sistema. Si HDB SQL OS User está configurado para acceder solo a la base de datos de tenant, se producirá un error en la operación de detección.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Resources** y seleccione SnapCenter Plug-in for SAP HANA Database en la lista.
  2. En la página **Recursos**, seleccione el tipo de recurso en la lista **Ver**.
  3. (Opcional) haga clic en y seleccione el nombre de host.

     A continuación, puede hacer clic en para cerrar el panel de filtros.
  4. Seleccione la base de datos y, a continuación, haga clic en **Configurar base de datos**.
  5. En la sección Configure database settings, introduzca una clave de almacenamiento de usuario seguro HDB.

     Se muestra el nombre de host del plugin y el usuario de sistema operativo SQL HDB se rellena automáticamente a <sid>-.
  6. Haga clic en **Aceptar**.

La configuración de la base de datos se puede modificar desde la página Topology.

## Descubra recursos y prepare contenedores de bases de datos multitenant para la protección de datos

**Detectar las bases de datos automáticamente**

Los recursos son bases de datos de SAP HANA y volumen de datos no data en el host Linux que gestiona SnapCenter. Puede añadir estos recursos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos SAP HANA disponibles.

**Lo que necesitará**

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir una clave de almacenamiento de usuario HDB, añadir hosts y configurar las conexiones del sistema de almacenamiento.
- Debe haber configurado la clave de almacenamiento de usuario seguro HDB y el usuario sistema operativo HDB SQL en el host Linux.

    - Debe configurar la clave de almacenamiento de usuario HDB con el usuario SID adm. Por ejemplo, para el sistema HANA con A22 como SID, la clave de almacenamiento de usuario HDB debe configurarse con a22adm.
- El plugin de SnapCenter para base de datos SAP HANA no es compatible con la detección automática de los recursos que residen en entornos virtuales RDM/VMDK. Debe proporcionar la información de almacenamiento para entornos virtuales al mismo tiempo que añade las bases de datos de forma manual.

**Acerca de esta tarea**

Después de instalar el plugin, todos los recursos en ese host Linux se detectan de forma automática y se muestran en la página Resources.

Los recursos de detección automática no se pueden modificar ni eliminar.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Resources** y seleccione el plugin para base de datos de SAP HANA en la lista.
  2. En la página **Recursos**, seleccione el tipo de recurso en la lista Ver.
  3. (Opcional) haga clic en y, a continuación, seleccione el nombre de host.

     A continuación, puede hacer clic en para cerrar el panel de filtros.
  4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

     Los recursos se muestran junto con cierta información, como el tipo de recurso, el nombre del host, los grupos de recursos asociados, el tipo de backup, las políticas y el estado general.

     - Si la base de datos se encuentra en un almacenamiento de NetApp y no está protegida, se muestra Not protected en la columna Overall Status.
     - Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, y si no se ejecuta una operación de backup, se muestra Not run en la columna Overall Status. El estado cambiará de otro modo a Backup failed o Backup succeeded según el estado de la última copia de seguridad.

Si la base de datos SAP HANA no tiene una clave de almacenamiento de usuario seguro HDB configurada, aparece un icono de candado rojo junto al recurso. Si durante una operación de detección posterior, se encontró que la clave de almacenamiento de usuario seguro HDB configurada era incorrecta o no proveía acceso a la base de datos, entonces el icono de candado rojo volverá a aparecer.

**Después de terminar**

Es necesario configurar la clave de almacenamiento de usuario seguro HDB y el usuario del sistema operativo HDBSQL para proteger la base de datos o añadirla al grupo de recursos para realizar operaciones de protección de datos.

"Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA"

**Prepare contenedores de bases de datos multitenant para la protección de datos**

Para los hosts SAP HANA registrados directamente en SnapCenter, instalar o actualizar

el plugin de SnapCenter para base de datos SAP HANA dará lugar a una detección automática de los recursos en el host. Después de instalar o actualizar el plugin, para cada recurso de contenedores de bases de datos multitenant (MDC) que se encontraba en el host del plugin, otro recurso de MDC se descubre automáticamente con un formato GUID diferente y se registra en SnapCenter. El nuevo recurso se encontrará en el estado «bloqueado».

**Acerca de esta tarea**

Por ejemplo, en SnapCenter 4.2, si el recurso de E90 MDC se encuentra en el host del plugin y se registró manualmente, después de actualizar a SnapCenter 4.3, se detecta otro recurso de E90 MDC con un GUID diferente y se registra en SnapCenter.

> Los backups asociados con el recurso de SnapCenter 4.2 y las versiones anteriores deben conservarse hasta que finalice el período de retención. Después de que caduque el período de retención, puede eliminar el recurso de MDC antiguo y continuar gestionando el nuevo recurso de MDC detectado automáticamente.

`Old MDC resource` Es el recurso MDC para un host de plugins que se añadió manualmente en SnapCenter 4.2 o versiones anteriores.

Ejecute los siguientes pasos para empezar a utilizar el nuevo recurso detectado en SnapCenter 4.3 para las operaciones de protección de datos:

- Pasos*

1. En la página **Recursos**, seleccione el antiguo recurso MDC con copias de seguridad añadidas a la versión anterior de SnapCenter, y colóquelo en "modo de mantenimiento" de la página Topology.

   Si el recurso forma parte de un grupo de recursos, coloque al grupo de recursos en «modo de mantenimiento».

2. Configure el nuevo recurso MDC detectado después de actualizar a SnapCenter 4.3. Para ello, seleccione el nuevo recurso de la página Resources.

   '"Nuevo recurso MDC'" es el recurso de MDC recientemente descubierto que se descubrió una vez que el servidor SnapCenter y el host del plugin se actualizaron a 4.3. El nuevo recurso MDC puede identificarse como un recurso con el mismo SID que el recurso MDC anterior, para un host dado, y con un icono de candado rojo junto a él en la página Resources.

3. Proteja el nuevo recurso MDC detectado después de actualizar a SnapCenter 4.3. Para ello, seleccione políticas de protección, programaciones y configuraciones de notificaciones.
4. Elimine los backups realizados en SnapCenter 4.2 o versiones anteriores según la configuración de retención.
5. Elimine el grupo de recursos en la página Topology.
6. Elimine el recurso MDC antiguo de la página Resources.

   Por ejemplo, si el período de retención de las copias de Snapshot primarias es de 7 días y la retención de copias de Snapshot secundarias es de 45 días, después de completar 45 días y después de eliminar todos los backups, debe eliminar el grupo de recursos y el recurso MDC antiguo.

**Más información**

"Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA"

"Consulte los backups y los clones de la base de datos SAP HANA en la página Topology"

## Añada recursos manualmente al host del plugin

La detección automática no es compatible con determinadas instancias de HANA. Debe añadir estos recursos manualmente.

### Lo que necesitará

Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, configurar conexiones del sistema de almacenamiento y añadir una clave de almacenamiento de usuario HDB.

### Acerca de esta tarea

La detección automática no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

> Si se detectan los recursos anteriores, las operaciones de protección de datos no son compatibles con estos recursos.

- Configuración de varios hosts DE HANA
- Replicación de sistemas HANA
- Varias instancias en el mismo host
- Pasos*

1. En el panel de navegación de la izquierda, seleccione el plugin de SnapCenter para base de datos SAP HANA en la lista desplegable y, a continuación, haga clic en **Resources**.
2. En la página **Recursos**, haga clic en **Agregar base de datos SAP HANA**.
3. En la página **proporcionar detalles del recurso**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Tipo de recurso | Introduzca el tipo de recurso. Los tipos de recurso son Single Container, Multitenant Database Container (MDC) y Non-data Volume. |
| Nombre del sistema HANA | Introduzca el nombre descriptivo del sistema SAP HANA. Esta opción solo está disponible si seleccionó los tipos de recursos Single Container o MDC. |
| SID | Introduzca el ID del sistema (SID). El sistema SAP HANA instalado se identifica por un SID exclusivo. |
| Host de plugin | Seleccione el host del plugin. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Claves de almacenamiento de usuario seguras HDB | Introduzca la clave para conectarse al sistema SAP HANA. La clave contiene la información de inicio de sesión para conectarse a la base de datos. |
| Usuario de sistema operativo de HDBSQL | Introduzca el nombre de usuario para el que se configuró la clave de almacenamiento de usuario seguro HDB. Para Windows, es obligatorio que el usuario de sistema operativo de HDBSQL sea el usuario SISTEMA. Por lo tanto, debe configurar la clave de almacenamiento de usuario seguro HDB para el usuario SISTEMA. |

4. En la página **Provide Storage Footprint**, seleccione un sistema de almacenamiento y elija uno o más volúmenes, LUN y qtrees; a continuación, haga clic en **Save**.

   Opcional: Puede hacer clic en el Icono para añadir más volúmenes, LUN y qtrees desde otros sistemas de almacenamiento.

5. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Las bases de datos se muestran junto con información como el SID, host del plugin, políticas y grupos de recursos asociados, y el estado general

Si desea proporcionar a los usuarios acceso a los recursos, debe asignar los recursos a los usuarios. De este modo, los usuarios pueden realizar las acciones para las cuales tienen permisos sobre los activos que les asignaron.

"Añada un usuario o grupo y asigne roles y activos"

Después de añadir las bases de datos, puede modificar los detalles de la base de datos SAP HANA.

La siguiente información no se puede modificar si el recurso SAP HANA tiene backups asociados:

- Contenedores de bases de datos multitenant (MDC): SID o host de HDBSQL Client (plugin)
- Contenedor único: Host de SID o cliente de HDBSQL (plugin)
- Volumen sin datos: Nombre del recurso, SID asociado o host del plugin

## Crear políticas de backup para bases de datos SAP HANA

Antes de usar SnapCenter para realizar un backup de los recursos de la base de datos SAP HANA, debe crear una política de backup para el recurso o grupo de recursos que desea incluir en el backup. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups.

**Lo que necesitará**

- Debe tener definida una estrategia de backup.

Para obtener más detalles, consulte cómo definir una estrategia de protección de datos para las bases de datos SAP HANA.

- Debe haberse preparado para la protección de datos completando tareas como instalar SnapCenter, añadir hosts, configurar las conexiones del sistema de almacenamiento y añadir recursos.
- El administrador de SnapCenter debe haberle asignado las instancias de SVM de los volúmenes de origen y de destino en caso de que replique copias de Snapshot en un reflejo o almacén.

  Además, puede definir la configuración de replicación, script y aplicaciones en la política. Estas opciones ahorran tiempo cuando se desea volver a utilizar la política con otro grupo de recursos.

- Pasos*

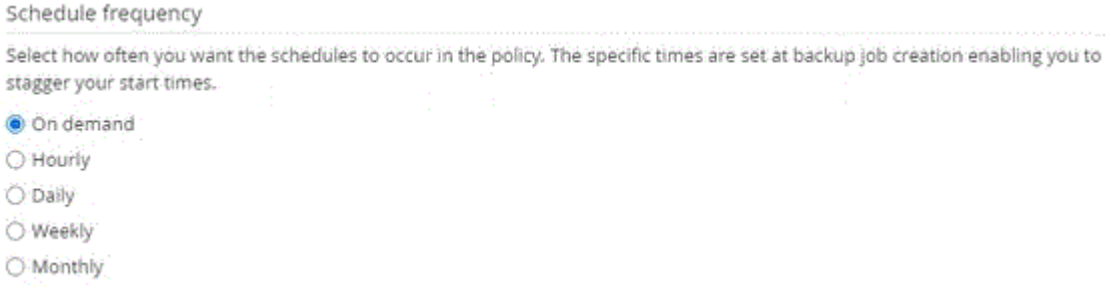
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página **Configuración**, haga clic en **Directivas**.
  3. Haga clic en **Nuevo**.
  4. En la página **Nombre**, introduzca el nombre y la descripción de la directiva.
  5. En la página **Configuración**, realice los siguientes pasos:

     - Elija el tipo de backup:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Realice una comprobación de integridad de la base de datos | Seleccione **copia de seguridad basada en archivos**. Solo se realiza un backup de los inquilinos activos. |
| Crear un backup mediante la tecnología de copia de Snapshot | Seleccione **Snapshot Based**. |

     - Especifique el tipo de programa seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

       Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de backup mientras crea un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de backup, pero también le permite asignar diferentes programaciones de backup a cada política.




Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

◦ En la sección **Configuración de copia de seguridad personalizada**, proporcione cualquier configuración de copia de seguridad específica que tenga que pasarse al plugin en formato de clave-valor.

Puede pasar varios pares de clave-valor al plugin.

1. En la página **Retention**, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página Tipo de copia de seguridad:

| Si desea… | Realice lo siguiente… |
|---|---|
| Conservar una cierta cantidad de copias de Snapshot | Seleccione **total Snapshot copies to keep** y, a continuación, especifique el número de copias Snapshot que desea conservar.<br><br>Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas.<br><br>El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.<br><br>Para los backups basados en copias de Snapshot, debe establecer el número de retención en 2 o más si va a habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino. |
| Conserve las copias de Snapshot por una cierta cantidad de días | Seleccione **mantener copias Snapshot para** y, a continuación, especifique el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas. |

2. Para las copias de seguridad basadas en copias de Snapshot, especifique la configuración de replicación en la página **replicación**:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Actualizar SnapMirror después de crear una copia Snapshot local** | Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror).<br><br>Si la relación de protección en ONTAP es del tipo reflejo y almacén y si selecciona solo esta opción, la copia de Snapshot creada en el origen no se transferirá al destino, pero sí aparecerá en el destino. Si esta copia de Snapshot se selecciona desde el destino para realizar una operación de restauración, entonces aparece el mensaje de error Secondary Location is not available for the selected vaulted/mirrored backup. |
| **Actualizar SnapVault después de crear una copia Snapshot local** | Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). |
| **Etiqueta de política secundaria** | Seleccione una etiqueta de Snapshot.<br><br>Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta.<br><br>Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria. |
| **Número de reintentos de error** | Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga. |

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear grupos de recursos y añadir políticas

Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación. Un grupo de recursos es necesario para cualquier trabajo de protección de datos. También debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, haga clic en **Nuevo grupo de recursos**.
3. En la página **Nombre**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba un nombre para el grupo de recursos.<br><br>El nombre del grupo de recursos no debe superar los 250 caracteres. |
| Etiquetas | Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.<br><br>Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta. |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.<br><br>Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |

4. En la página **Recursos**, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

   Esto permite filtrar información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.

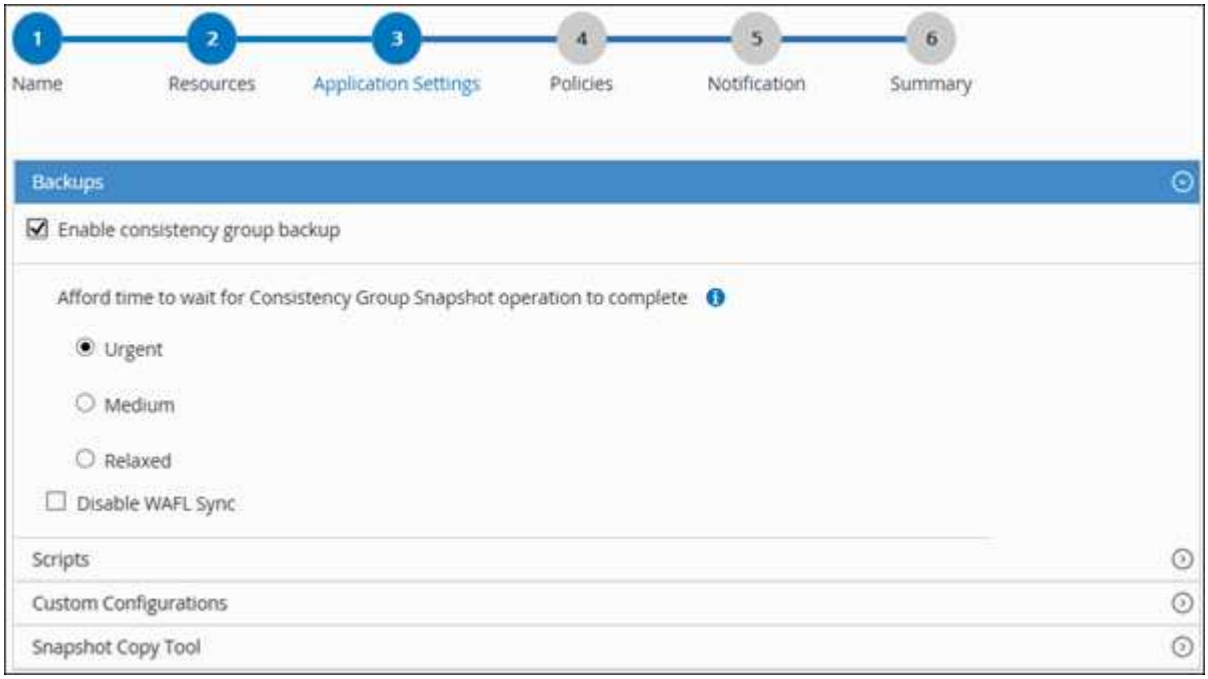
6. En la página **Configuración de la aplicación**, haga lo siguiente:

   a. Haga clic en la flecha **copias de seguridad** para establecer las opciones de copia de seguridad adicionales:

      Habilite el backup del grupo de consistencia y realice las siguientes tareas:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Permitir que se complete la operación de snapshot del grupo de consistencia | Seleccione **Urgent**, **Medium** o **Relaxed** para especificar el tiempo de espera para completar la operación de copia snapshot.<br><br>Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos. |
| Deshabilite la sincronización WAFL | Seleccione este campo para evitar forzar un punto de coherencia de WAFL. |

+




   a. Haga clic en la flecha **Scripts** e introduzca los comandos previos y posteriores para las operaciones de inactividad, copia snapshot y reanudación. También puede escribir los comandos previos para que se ejecuten antes de salir en caso de un fallo.

   b. Haga clic en la flecha **configuraciones personalizadas** e introduzca los pares personalizados clave-valor requeridos para todas las operaciones de protección de datos que utilizan este recurso.

| Parámetro | Ajuste | Descripción |
|---|---|---|
| ARCHIVE_LOG_ENABLE | (S/N) | Permite la gestión del registro de archivos para eliminar los registros de archivos. |

| Parámetro | Ajuste | Descripción |
|---|---|---|
| RETENCIÓN_LOG_ARCHIVO | número_de_días | Especifica la cantidad de días que se conservan los registros de archivo.<br><br>Este valor debe ser igual o mayor que las RETENTIONS NTAP_SNAPSHOT_. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Especifica la ruta de acceso al directorio que contiene los registros de archivo. |
| ARCHIVO_LOG_EXT | extensión_archivo | Especifica la longitud de la extensión del archivo de registro de archivos.<br><br>Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.1615185 51942 9 y si el valor file_extension es 5, la extensión del registro conservará 5 dígitos, que son 16151. |
| ARCO ARCHIVE_LOG_RECURSIVE_ SE | (S/N) | Permite la gestión de registros de ficheros en subdirectorios.<br><br>Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios. |

Los pares personalizados de clave-valor son compatibles con los sistemas del plugin de SAP HANA Linux y no son compatibles con la base de datos SAP HANA registrada como un plugin de Windows centralizado.

c. Haga clic en la flecha **Snapshot Copy Tool** para seleccionar la herramienta que permite crear copias Snapshot:

| Si desea que… | Realice lo siguiente… |
|---|---|
| SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente antes de crear una copia de Snapshot. En el caso de recursos de Linux, esta opción no es aplicable. | Seleccione **SnapCenter with File System Consistency**.<br><br>Esta opción no es aplicable para el plugin de SnapCenter para la base de datos SAP HANA. |
| SnapCenter cree una copia de Snapshot en el nivel del almacenamiento | Seleccione **SnapCenter sin coherencia del sistema de archivos**. |

| Si desea que… | Realice lo siguiente… |
| --- | --- |
| Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot. | Seleccione **otros** y, a continuación, escriba el comando que se ejecutará en el host para crear una copia Snapshot. |

7. En la página **Directivas**, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

   También puede crear una directiva haciendo clic en + .

   Las políticas figuran en la sección Configure schedules for selected policies.

   b. En la columna Configure Schedules, haga clic en + para la directiva que desea configurar.

   c. En el cuadro de diálogo Agregar programas para la directiva *policy_name* , configure la programación y, a continuación, haga clic en **Aceptar**.

   Policy_name es el nombre de la política seleccionada.

   Los horarios configurados se enumeran en la columna **programas aplicados**.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

1. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Realice un backup de las bases de datos SAP HANA

Si un recurso aún no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

**Lo que necesitará**

- Debe tener creada una política de backup.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Para realizar una operación de backup basada en copia de Snapshot, asegúrese de que todas las bases de datos de tenant sean válidas y estén activas.
- Si desea crear un backup basado en archivos cuando una o varias bases de datos de tenant están inactivos, establezca el parámetro

ALLOW_FILE_BASED_BACKUP_IFINACTIVE_ARRENDATARIOS_PRESENT en **YES** en el archivo de propiedades de HANA con el cmdlet Set-SmConfigSettings.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software"

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **recurso**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Haga clic en y luego seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.
3. Haga clic en el recurso que desea incluir en el backup.
4. En la página **recurso**, seleccione **usar formato de nombre personalizado para copia Snapshot** y, a continuación, escriba un formato de nombre personalizado que desee utilizar para el nombre de copia Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.
5. En la página **Configuración de la aplicación**, haga lo siguiente:

   - Haga clic en la flecha **copias de seguridad** para establecer las opciones de copia de seguridad adicionales:

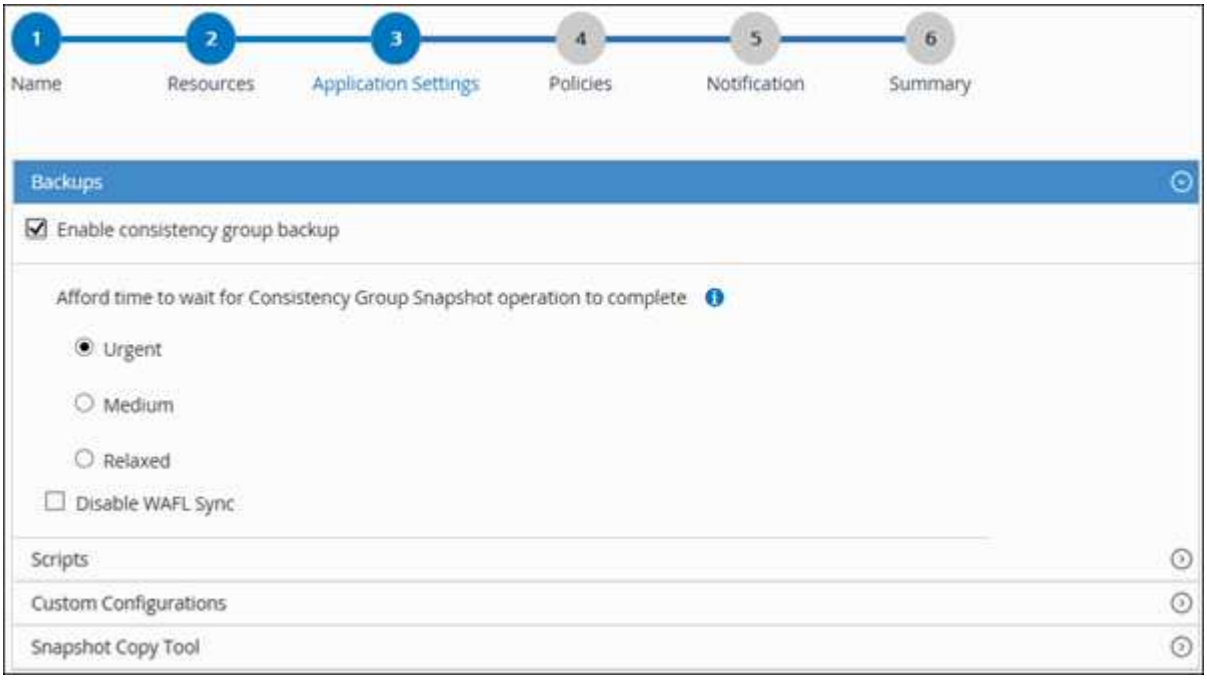
     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Permitir que se complete la operación de "Snapshot de grupo de consistencia" | Seleccione **Urgent**, **Medium** o **Relaxed** para especificar el tiempo de espera para que termine la operación de copia snapshot. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos. |
| Deshabilite la sincronización WAFL | Seleccione este campo para evitar forzar un punto de coherencia de WAFL. |

   - Haga clic en la flecha **Scripts** para ejecutar comandos previos y posteriores para la pausa, la copia de Snapshot y la reanudación de la copia.

     También puede ejecutar los comandos previos antes de salir de la operación de backup. Los scripts previos y posteriores se ejecutan en el servidor de SnapCenter.
   - Haga clic en la flecha **Custom Configurations**y, a continuación, escriba las parejas de valor personalizadas necesarias para todos los trabajos que utilicen este recurso.
   - Haga clic en la flecha **Snapshot Copy Tool** para seleccionar la herramienta que permite crear copias Snapshot:

| Si desea que… | Realice lo siguiente… |
| --- | --- |
| SnapCenter cree una copia de Snapshot a nivel del almacenamiento | Seleccione **SnapCenter sin coherencia del sistema de archivos**. |
| SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente para luego crear una copia de Snapshot | Seleccione **SnapCenter with File System Consistency**. |
| Se escriba el comando para crear una copia de Snapshot | Seleccione **otros** y, a continuación, escriba el comando para crear una copia Snapshot. |




6. En la página **Directivas**, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

   También puede crear una directiva haciendo clic en + .

   En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   a. Haga clic en + En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

   b. En el cuadro de diálogo Agregar programas para la directiva *policy_name* , configure la programación y, a continuación, haga clic en **Aceptar**.

      *policy_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

1. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de los recursos.

3. Haga clic en **copia de seguridad ahora**.
4. En la página **copia de seguridad**, realice los siguientes pasos:
   a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.
   - En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

     Para obtener más información, consulte: "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"

   - Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup.

     Para aumentar el tamaño de pila de Java, busque el archivo de script */opt/netapp/init_scripts/svservice*. En ese script, el comando *do_start method* inicia el servicio de complemento de VMware de SnapCenter. Actualice este comando a lo siguiente: *Java -jar -Xmx8192M -Xms4096M*

## Realice un backup de los grupos de recursos

Un grupo de recursos es una agrupacion de recursos en un host. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

### Lo que necesitará

- Debe tener creado un grupo de recursos con una política anexada.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".

### Acerca de esta tarea

Puede hacer una copia de seguridad de un grupo de recursos bajo demanda desde la página **Recursos**. Si un

grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en y, a continuación, seleccione la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos SAP HANA

Es posible crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar cmdlets de PowerShell para realizar backup, restaurar o clonar bases de datos SAP HANA.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

  No debe haber instalaciones de complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

  SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de datos única.

- Pasos*

1. Inicie una sesión de conexión de PowerShell con mediante el cmdlet Open-SmConnection.

```
PS C:\> Open-SmStorageConnection
```

2. Cree una nueva conexión con el sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Cree una credencial nueva mediante el cmdlet Add-SmCredential.

   Este ejemplo muestra cómo crear una nueva credencial llamada FinanceAdmin con las credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Añada el host de comunicación de SAP HANA a servidor SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Instale el paquete y el plugin de SnapCenter para base de datos SAP HANA en el host.

   Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61
-ApplicationCode hana
```

   Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina la ruta al cliente de HDBSQL.

   Para Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61
-PluginCode hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

Para Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Realizar un backup de bases de datos mediante cmdlets de PowerShell

Realizar un backup de una base de datos incluye establecer una conexión con SnapCenter Server, añadir recursos, añadir una política, crear un grupo de recursos de backup y realizar backups.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe añadir la conexión con el sistema de almacenamiento y crear una credencial.
- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
   ```

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada los recursos mediante el cmdlet Add-SmResources.

   Este ejemplo muestra cómo añadir una base de datos SAP HANA del tipo SingleContainer:

   ```
   C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
   -DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
   (@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"
   }) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
   'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
   ```

   Este ejemplo muestra cómo añadir una base de datos SAP HANA del tipo MultipleContainers:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.neta
pp.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

Este ejemplo muestra cómo crear un recurso de volúmenes sin datos:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.

   Este ejemplo crea una política de backup para un backup basado en copias de Snapshot:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
   -PluginPolicyType hana -BackupType SnapShotBasedBackup
   ```

   Este ejemplo crea una política de backup para un backup basado en archivos:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
   -PluginPolicyType hana -BackupType FileBasedBackup
   ```

4. Proteja el recurso o añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

   Este ejemplo protege un recurso de contenedor único:

   ```
   C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
   hana_snapshotbased,hana_Filebased
    -Resources @{"Host"="host.example.com";"UID"="SID"} -Description
   test -usesnapcenterwithoutfilesystemconsistency
   ```

   Este ejemplo protege un recurso de varios contenedores:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

En este ejemplo, se crea un nuevo grupo de recursos con la política y los recursos especificados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="scc
orelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Este ejemplo crea un grupo de recursos de volumen sin datos:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="
hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Plug
inName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDa
taVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

   Este ejemplo muestra cómo realizar un backup de un grupo de recursos:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   Este ejemplo realiza un backup de un recurso protegido:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"} -Policy
hana_Filebased
```

1. Supervise el estado de la tarea (running, completed o failed) mediante el cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

2. Supervise los detalles del trabajo de backup como ID de backup, nombre de backup para realizar una operación de restauración o clonado mediante el cmdlet Get-SmBackupReport.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Supervisar las operaciones de backup

### Supervisar las operaciones de backup de las bases de datos SAP HANA

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

#### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Jobs**.
3. En la página Jobs, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
   d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
   e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

   Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

### Supervise las operaciones de protección de datos en bases de datos SAP HANA en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también muestra información sobre la operación de propagación.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

   Al hacer clic en una de las operaciones, se muestran sus detalles en la página Job Details.

## Consulte los backups y los clones de la base de datos SAP HANA en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario.

### Acerca de esta tarea

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
- Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.
- Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

  La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

Los clones de un backup de un reflejo con versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejo no incluye el backup con versión flexible.

En la página **Topology**, puede ver todas las copias de seguridad y clones disponibles para el recurso o grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página **Recursos**, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
  3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

     Si el recurso está protegido, se muestra la página con el resumen seleccionado.

  4. Consulte **Summary Card** para ver un resumen del número de copias de seguridad y clones disponibles en el almacenamiento principal y secundario.

     La sección **Tarjeta de resumen** muestra el número total de copias de seguridad basadas en archivos, copias de seguridad de instantáneas y clones.

Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

1. En la vista **Administrar copias**, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

   Estos detalles se muestran en forma de tabla.

2. Seleccione el backup de la tabla y, a continuación, haga clic en los iconos de protección de datos para llevar a cabo operaciones de restauración, clonado y eliminación.

   Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

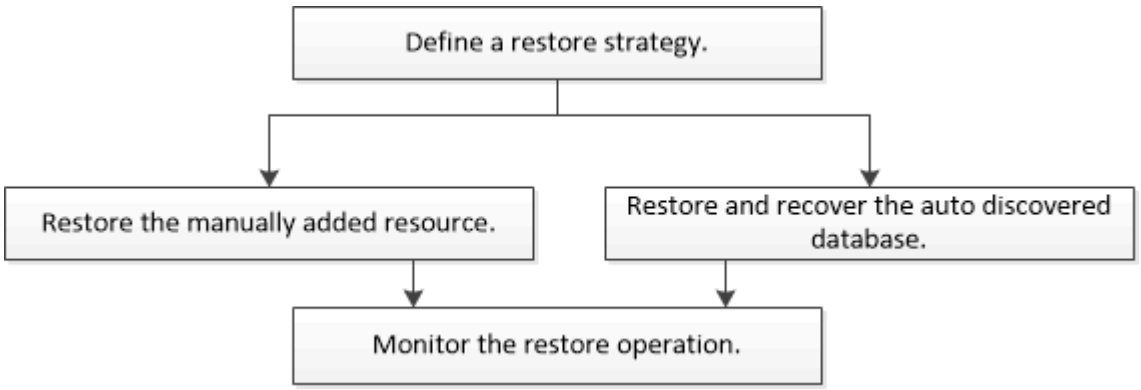
3. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
4. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

# Restaure bases de datos de SAP HANA

## Restaure el flujo de trabajo

El flujo de trabajo de restauración y recuperación incluye planificar, realizar las operaciones de restauración y supervisarlas.

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de restauración:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen detalles sobre los cmdlets de PowerShell.

"Guía de referencia de cmdlets de SnapCenter Software".

## Restaurar y recuperar un backup de recurso añadido manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

### Lo que necesitará

- Debe tener un backup de los recursos o del grupo de recursos.

- Cancele la operación de backup que se encuentra en curso y que corresponde al recurso o grupo de recursos que desea restaurar.

**Acerca de esta tarea**

- Las copias de backup basadas de archivos no se pueden restaurar desde SnapCenter.
- Después de actualizar a SnapCenter 4.3, se pueden restaurar los backups realizados en SnapCenter 4.2, pero no se pueden recuperar. Para recuperar los backups realizados en SnapCenter 4.2, debe usar el estudio HANA o secuencias de comandos de recuperación HANA externas a SnapCenter.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Los recursos se muestran junto con el tipo, el host, las políticas y los grupos de recursos asociados, y el estado.

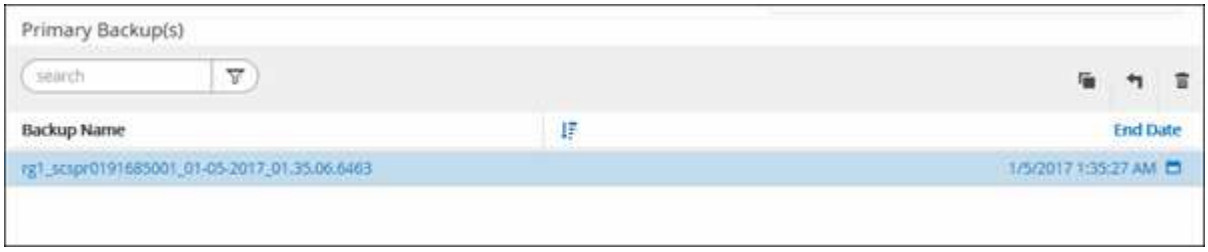
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   Si el recurso no está protegido, se muestra "'no protegido'" en la columna Estado general. Esto significa que el recurso no está protegido o que otro usuario hizo el backup de este recurso.

3. Seleccione el recurso o seleccione un grupo de recursos y, a continuación, seleccione un recurso de ese grupo.

   Se muestra la página con el resumen.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. En la tabla de backups primarios, seleccione el backup desde el cual quiere restaurar y, a continuación, haga clic en .




6. En la página **Restore Scope**, seleccione **Complete Resource** o **File Level**.
   a. Si selecciona **Complete Resource**, se restauran todos los volúmenes de datos configurados de la base de datos SAP HANA.

      Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

b. Si selecciona **nivel de archivo**, puede seleccionar **todo** o seleccionar los volúmenes o qtrees específicos y, a continuación, introducir la ruta relacionada con esos volúmenes o qtrees, separados por comas

- Puede seleccionar varios volúmenes y qtrees.
- Si el tipo de recurso es LUN, se restaura todo el LUN.

  Puede seleccionar varios LUN.

Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.

1. En la página **Pre OPS**, escriba los comandos previos a la restauración y los comandos de desmontaje que se ejecutarán antes de realizar un trabajo de restauración.

   Los comandos de desmontaje no están disponibles para los recursos de detección automática.

2. En la página **Post OPS**, escriba los comandos Mount y post restore que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

3. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en la página **Ajustes** > **Ajustes globales**.

4. Revise el resumen y, a continuación, haga clic en **Finalizar**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Restaurar y recuperar un backup de base de datos detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

### Lo que necesitará

- Debe tener un backup de los recursos o del grupo de recursos.
- Cancele la operación de backup que se encuentra en curso y que corresponde al recurso o grupo de recursos que desea restaurar.

### Acerca de esta tarea

- Las copias de backup basadas de archivos no se pueden restaurar desde SnapCenter.
- Después de actualizar a SnapCenter 4.3, se pueden restaurar los backups realizados en SnapCenter 4.2, pero no se pueden recuperar. Para recuperar los backups realizados en SnapCenter 4.2, debe usar el estudio HANA o secuencias de comandos de recuperación HANA externas a SnapCenter.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

Los recursos se muestran junto con el tipo, el host, las políticas y los grupos de recursos asociados, y el estado.

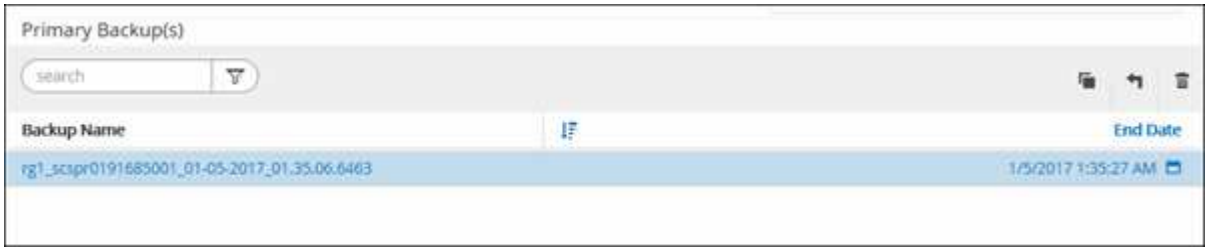
Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

Si el recurso no está protegido, se muestra "'no protegido'" en la columna Estado general. Esto significa que el recurso no está protegido o que otro usuario hizo el backup de este recurso.

3. Seleccione el recurso o seleccione un grupo de recursos y, a continuación, seleccione un recurso de ese grupo.

   Se muestra la página con el resumen.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. En la tabla de backups primarios, seleccione el backup desde el cual quiere restaurar y, a continuación, haga clic en .




6. En la página **Restore Scope**, seleccione **Complete Resource** para restaurar los volúmenes de datos configurados de la base de datos SAP HANA.

   Puede seleccionar **Complete Resource** (con o sin **Volume Revert**) o **Inquilino**.

   El servidor SnapCenter no admite la operación de recuperación para varios inquilinos cuando el usuario selecciona la opción **base de datos de inquilinos** o **Restaurar completa**. Debe usar HANA Studio o el script HANA python para realizar la operación de recuperación.

   a. Seleccione **revertir volumen** si desea restaurar todo el volumen.

      Esta opción está disponible para backups realizados en SnapCenter 4.3 en entornos NFS.

      Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina. Esto se aplica cuando se selecciona la opción **Complete Resource** with **Volume Revert** para restaurar.

   b. Seleccione **base de datos de arrendatario**.

      Esta opción solo está disponible para recursos MDC.

   Asegúrese de detener la base de datos de tenant antes de realizar la operación de restauración.

Si selecciona la opción **base de datos de inquilino**, debe usar HANA Studio o utilizar secuencias de

comandos de recuperación de HANA externas a SnapCenter para realizar la operación de recuperación.

1. En la página **alcance de recuperación**, seleccione una de las siguientes opciones:

| Si… | Realice lo siguiente… |
| --- | --- |
| Desea recuperar el mayor cierre posible a la hora actual | Seleccione **recuperar al estado más reciente**. Para los recursos de contenedor único, especifique una o más ubicaciones de backup de registro y catálogo.<br><br>Para los recursos de contenedor de base de datos multitenant (MDC) especifican una o varias ubicaciones de backup de registros y la ubicación del catálogo de backups.<br><br>Para los recursos del MDC, la ruta de acceso debe contener tanto registros de la base de datos del sistema como de la base de datos de tenant. |

| Si… | Realice lo siguiente… |
| --- | --- |
| Desea recuperar al punto en el tiempo especificado | Seleccione **Recover to point in time**.<br><br>a. Seleccione la zona horaria.<br><br>De forma predeterminada, la zona horaria del navegador se completa.<br><br>La zona horaria seleccionada junto con la hora de entrada se convierte en GMT absoluta.<br><br>b. Introduzca la fecha y la hora. Por ejemplo, el host Linux para HANA se encuentra en Sunnyvale, CA y el usuario en Raleigh, NC está recuperando los registros en SnapCenter.<br><br>La diferencia horaria entre ambas ubicaciones es de 3 horas, y como el usuario ha iniciado sesión en Raleigh, NC, la zona horaria predeterminada del navegador que se seleccionará en la GUI es GMT-04:00.<br><br>Si el usuario desea realizar una recuperación a 5:07 a.m .Sunnyvale, CA, el usuario debe configurar la zona horaria del navegador para la zona horaria del host Linux de HANA, que es GMT-00 y especificar la fecha y la hora como 5:00 a.m.<br><br>Para los recursos de contenedor único, especifique una o más ubicaciones de backup de registro y catálogo.<br><br>Para los recursos MDC, especifique una o más ubicaciones de backup de registros y la ubicación del catálogo de backups.<br><br>Para los recursos del MDC, la ruta de acceso debe contener tanto registros de la base de datos del sistema como de la base de datos de tenant. |
| Desea recuperar a un backup de datos específico | Seleccione **Recover to specified data backup**. |
| No desea recuperar | Seleccione **sin recuperación**. La operación de recuperación debe realizarse manualmente desde el estudio HANA. |

Solo es posible recuperar los backups que se realizan después de la actualización a SnapCenter 4.3, siempre y cuando el host y el plugin se actualicen a SnapCenter 4.3 y los backups seleccionados para

la restauración se tomen después de que el recurso se convierta o se detecte como recurso automático.

2. En la página **Pre OPS**, escriba los comandos previos a la restauración y los comandos de desmontaje que se ejecutarán antes de realizar un trabajo de restauración.

   Los comandos de desmontaje no están disponibles para los recursos de detección automática.

3. En la página **Post OPS**, escriba los comandos Mount y post restore que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

4. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en la página **Ajustes** > **Ajustes globales**.

5. Revise el resumen y, a continuación, haga clic en **Finalizar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Restaurar una base de datos SAP HANA mediante cmdlets de PowerShell

La restauración de un backup de base de datos SAP HANA incluye iniciar una sesión de conexión con SnapCenter Server, mostrar una lista de backups y recuperar información de los backups, así como restaurar un backup.

**Lo que necesitará**

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Identifique el backup que desea restaurar mediante los cmdlets Get-SmBackup y Get-SmBackupReport.

   Este ejemplo muestra que hay dos backups disponibles para restaurar:

```
 PS C:\> Get-SmBackup

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM  Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

En este ejemplo, se muestra información detallada sobre el backup del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Inicie el proceso de recuperación en el estudio HANA.

   La base de datos se cierra.

4. Puede restaurar los datos del backup mediante el cmdlet Restore-SmBackup.

   AppObjectId es "Host\Plugin\UID", donde UID = SID es para un recurso de tipo de contenedor único y UID = MDC\SID es para un recurso de varios contenedores. Puede obtener el ResourceID a partir del cmdlet Get-smResources.

   ```
   Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
   ```

   Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento primario:

   ```
   Restore-SmBackup -PluginCode HANA -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 3
   ```

   Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento secundario:

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

+
Los backups estarán disponibles en el estudio HANA para recuperación.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Supervisar las operaciones de restauración de bases de datos SAP HANA

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

### Acerca de esta tarea

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente

- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

# Clonar backups de recursos SAP HANA

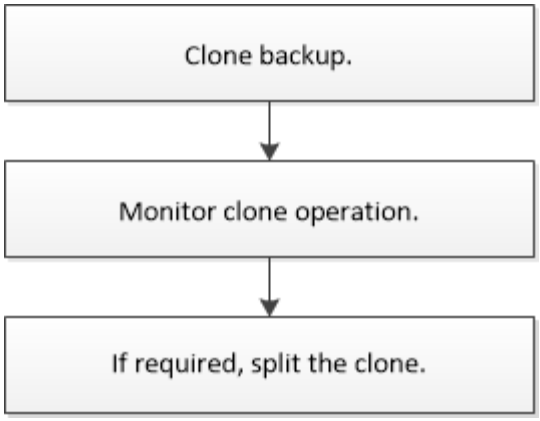
## Flujo de trabajo de clonado

El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

### Acerca de esta tarea

- Puede clonar en el servidor SAP HANA de origen.
- Es posible clonar backups de recursos por los siguientes motivos:
  - Para probar la funcionalidad que debe implementarse mediante la estructura de recursos actuales y el contenido durante los ciclos de desarrollo de aplicaciones
  - Para herramientas de manipulación y extracción de datos cuando se rellenan almacenes de datos
  - Para recuperar datos que se eliminaron o se modificaron por error

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de clonado:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen detalles sobre los cmdlets de PowerShell.

## Clonar un backup de base de datos SAP HANA

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario.

**Lo que necesitará**

- Debe tener un backup de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- No puede clonar backups basados en archivos.
- El servidor de clones de destino debe tener el mismo SID de instancia de SAP HANA que se proporciona en el campo SID de clon de destino.

**Acerca de esta tarea** para obtener información acerca de las limitaciones de la operación de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

     Los recursos se muestran junto con cierta información, como el tipo, el host, las políticas y los grupos de recursos asociados, y el estado.
  3. Seleccione el recurso o el grupo de recursos.

     Debe seleccionar un recurso para seleccionar un grupo de recursos.

     Se muestra la página con el resumen o grupo de recursos.
  4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
  5. Seleccione el backup de datos de la tabla y haga clic en .

6. En la página **ubicación**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Host de plugin | Seleccione el host en el que se debe alojar el clon y está instalado el plugin. |
| SID del clon de destino | Introduzca el ID de instancia de SAP HANA que se va a clonar desde los backups existentes. |
| Dirección IP de exportación NFS | Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados. |
| Iniciador iSCSI | Introduzca el nombre del iniciador de iSCSI del host al que se van a exportar los LUN. Esta opción está disponible solo si seleccionó el tipo de recurso LUN. |
| Protocolo | Introduzca el protocolo de LUN. Esta opción está disponible solo si seleccionó el tipo de recurso LUN. |

Si el recurso seleccionado es un LUN y lo clona desde un backup secundario, entonces se enumeran los volúmenes de destino. Un único recurso puede tener varios volúmenes de destino.

Antes de la clonado, debe asegurarse de que el iniciador de iSCSI o FCP estén presentes y estén configurados y conectados a hosts alternativos.

7. En la página **Scripts**, realice los siguientes pasos:

Los scripts se ejecutan en el host del plugin.

a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.
   - Comando previo a la clonado: Elimine las bases de datos existentes con el mismo nombre
   - Comando posterior a la clonado: Verifique o inicie una base de datos.
b. Escriba el comando de montaje para montar un sistema de archivos en un host.

   Comando de montaje para un volumen o qtree en un equipo Linux:

Ejemplo para NFS:

```
mount VSERVER_DATA_IP:%{VOLUME_NAME_Clone} /mnt
```

8. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Clonar backups de la base de datos SAP HANA mediante cmdlets de PowerShell

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Recupere los backups para realizar la operación de clonado mediante el cmdlet Get-SmBackup.

   Este ejemplo muestra que hay dos backups disponibles para clonar:

```
 C:\PS> Get-SmBackup

        BackupId                      BackupName
BackupTime                    BackupType
        --------                      ----------
----------                    ----------
         1                     Payroll Dataset_vise-f6_08... 8/4/2015
11:02:32 AM          Full Backup
         2                     Payroll Dataset_vise-f6_08... 8/4/2015
11:23:17 AM
```

3. Inicie una operación de clonado a partir de un backup existente y especifique las direcciones IP de exportación de NFS a las que se van a exportar los volúmenes clonados.

   Este ejemplo muestra que el backup que se va a clonar tiene una dirección NFSExportIPs de 10.232.206.169:

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

Si no se especificó NFSExportIPs, el valor predeterminado se exporta al host de destino del clon.

4. Compruebe que los backups se hayan clonado correctamente mediante el cmdlet Get-SmCloneReport para ver los detalles del trabajo de clonado.

   Puede ver detalles como el ID del clon, la fecha y hora de inicio, y la fecha y hora de finalización.

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

## Supervise las operaciones de clonado de base de datos SAP HANA

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

**Acerca de esta tarea**

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **trabajos**, realice los siguientes pasos:
     a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
     b. Especifique las fechas de inicio y finalización.
     c. En la lista desplegable **Tipo**, seleccione **Clonar**.
     d. En la lista desplegable **Estado**, seleccione el estado del clon.
     e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
  4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Divida un clon

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

### Acerca de esta tarea

- No se puede ejecutar la operación de división de clones en un clon intermedio.

  Por ejemplo, después de crear el clon 1 a partir de un backup de la base de datos, puede realizar un backup del clon 1 y luego clonar este backup (que sería el clon 2). Una vez creado el clon 2, el clon 1 se convierte en un clon intermedio y la operación de división de clones puede hacerse con el clon 1. No obstante, esta operación también puede ejecutarse con el clon 2.

  Después de dividir el clon 2, puede ejecutar la operación de división de clones con el clon 1, ya que este deja de ser el clon intermedio.

- Cuando divide un clon, se eliminan las copias de backup y los trabajos de clonado del clon.
- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Asegúrese de que el volumen o el agregado del sistema de almacenamiento estén en línea.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione la opción adecuada en la lista Ver:

| Opción | Descripción |
| --- | --- |
| Para aplicaciones de base de datos | Seleccione **base de datos** en la lista View. |
| Para sistemas de archivos | Seleccione **Ruta** en la lista Ver. |

3. Seleccione el recurso adecuado de la lista.

   Se muestra la página con el resumen.

4. En la vista Manage Copies, seleccione el recurso clonado (por ejemplo, la base de datos o el LUN) y, a continuación, haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
6. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

   La operación de división de clones se detiene si se reinicia el servicio de SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clones y luego volver a intentar la operación de división de clones.

   Si necesita más o menos tiempo de sondeo para comprobar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer un intervalo para que SMCore sondee el estado de la operación de división de clones. El valor se registra en milisegundos; el predeterminado son 5 minutos.

   Por ejemplo:

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

+
Se produce un error en la operación de inicio de división de clones si hay un backup, una restauración u otra división de clones en curso. Solo debe reiniciar la operación de división de clones una vez que hayan finalizado las operaciones en ejecución.

**Más información**

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

## Elimine o divida los clones de las bases de datos SAP HANA después de actualizar SnapCenter

Después de actualizar a SnapCenter 4.3, ya no se muestran los clones. Puede eliminar el clon o dividir los clones desde la página Topology del recurso desde el cual se crearon los clones.

**Acerca de esta tarea**

Si desea localizar el espacio de almacenamiento de los clones ocultos, ejecute el siguiente comando: `Get-SmClone -ListStorageFootprint`

- Pasos*
  1. Elimine los backups de los recursos clonados con el cmdlet remove-smbackup.
  2. Elimine el grupo de recursos de los recursos clonados mediante el cmdlet remove-smresourcegroup.
  3. Quite la protección del recurso clonado mediante el cmdlet remove-smprotectresource.
  4. Seleccione el recurso padre en la página **Recursos**.

     Se muestra la página con el resumen.
  5. En la vista **Manage Copies**, seleccione los clones de los sistemas de almacenamiento principal o secundario (reflejado o replicado).
  6. Seleccione los clones y, a continuación, haga clic en para eliminar clones o haga clic en para dividir los clones.
  7. Haga clic en **Aceptar**.

# Proteger bases de datos de Oracle

## Información general del plugin de SnapCenter para base de datos de Oracle

### Qué puede hacer con el plugin para base de datos de Oracle

El plugin de SnapCenter para bases de datos de Oracle es un compenente de NetApp SnapCenter Software que se instala en los hosts de Oracle que permite la gestión de protección de datos para aplicaciones de bases de datos de Oracle.

El plugin para bases de datos de Oracle automatiza las operaciones de backup, catalogación y descatalogación con Oracle Recovery Manager (RMAN), verificación, montaje, desmontaje, restauración, Recuperación y clonado de bases de datos de Oracle en el entorno de SnapCenter. El plugin para bases de datos de Oracle instala el plugin de SnapCenter para UNIX para realizar todas las operaciones de protección de datos.

Es posible utilizar el plugin para bases de datos de Oracle para gestionar backups de bases de datos de Oracle que ejecutan aplicaciones SAP. Sin embargo, no se admite la integración con BR*Tools de SAP.

- Realizar backup de archivos de datos, archivos de control y archivos de registro de archivo.

  El backup solo puede usarse en el nivel de la base de datos del contenedor (CDB).

- Restaurar y recuperar bases de datos, bases de datos de contenedor y bases de datos conectables (PDB).

  No se admite la recuperación incompleta de bases de datos conectables.

- Crear clones de bases de datos de producción hasta un momento específico.

  La clonado solo puede usarse en el nivel de la base de datos de contenedor.

- Verificar backups de inmediato.
- Montaje y desmontaje de datos y backups de registro para la operación de recuperación.
- Programar operaciones de backup y verificación.
- Supervisar todas las operaciones.
- Ver informes para operaciones de backup, restauración y clonado.

### Funciones del plugin para base de datos de Oracle

El plugin para bases de datos de Oracle se integra con la base de datos de Oracle en el host Linux o AIX y con las tecnologías de NetApp en el sistema de almacenamiento.

- Interfaz gráfica de usuario unificada

  La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar operaciones de backup, restauración, recuperación y clonado consistentes entre plugins, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins.

- Administración central automatizada

  Es posible programar operaciones de backup y clonado, configurar retención de backup basado en políticas y realizar operaciones de restauración. También es posible supervisar de manera proactiva el entorno configurando SnapCenter para que envíe alertas por correo electrónico.

- Tecnología de copia de Snapshot de NetApp no disruptiva

  SnapCenter utiliza la tecnología de copia de Snapshot de NetApp con el plugin para bases de datos de Oracle y el plugin para UNIX con el fin de realizar backups de bases de datos. Las copias de Snapshot consumen un espacio de almacenamiento mínimo.

El plugin para bases de datos de Oracle también ofrece los siguientes beneficios:

- Compatibilidad con backup, restauración, clonado, montaje, desmontaje y flujos de trabajo de verificación
- Detección automática de las bases de datos de Oracle configuradas en el host
- Compatibilidad para catalogar y descatalogar con Oracle RMAN
- Seguridad compatible con RBAC y delegación de roles centralizada

  También es posible configurar las credenciales para que los usuarios de SnapCenter autorizados tengan permisos en el nivel de las aplicaciones.

- Creación de copias de bases de datos de producción con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

  Se requiere una licencia de FlexClone en el sistema de almacenamiento donde desea crear el clon.

- Compatibilidad con la función del grupo de consistencia (CG) de ONTAP como parte de la creación de backups en entornos DE SAN y ASM
- Verificación de backups no disruptiva y automatizada
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de bases de datos

  En una sola operación se consolidan copias de Snapshot cuando las bases de datos en un solo host comparten el mismo volumen.

- Compatibilidad con infraestructuras físicas y virtualizadas
- Compatibilidad con NFS, iSCSI, Fibre Channel (FC), RDM, VMDK sobre NFS y VMFS, y ASM sobre NFS, SAN, RDM y VMDK
- Compatibilidad con la función de asignación de LUN selectiva (SLM) de ONTAP

  Habilitada de forma predeterminada, la función SLM detecta periódicamente los LUN que no poseen rutas optimizadas y los corrige. Puede configurar SLM mediante la modificación de los parámetros del archivo scu.properties ubicado en /var/opt/snapcenter/scu/etc.

  - Para deshabilitar esto, debe configurarse el valor de ENABLE_LUNPATH_MONITORING como false.
  - Es posible especificar la frecuencia en la cual se corrigen automáticamente las rutas de LUN mediante la asignación del valor (en horas) como LUNPATH_MONITORING_INTERVAL. Para obtener más información sobre SLM, consulte "Guía de administración de SAN de ONTAP 9".

## Tipos de almacenamiento compatibles con el plugin para bases de datos de Oracle

SnapCenter admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Debe comprobar la compatibilidad de su tipo de almacenamiento antes de instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX.

SnapCenter no es compatible con el aprovisionamiento de almacenamiento para Linux y AIX.

### Tipos de almacenamiento compatibles con Linux

En la siguiente tabla, se enumeran los tipos de almacenamiento admitidos en Linux.

| Máquina | Tipo de almacenamiento |
|---|---|
| Servidor físico | • LUN conectados a FC<br>• LUN conectados a iSCSI<br>• Volúmenes conectados en NFS |
| VMware ESXi | • Los LUN de RDM conectados por un HBAScanning de adaptadores de bus de host (HBA) FC o iSCSI pueden tardar mucho en completarse debido a que SnapCenter analiza todos los adaptadores de bus de host presentes en el host.<br><br>Puede editar el archivo **LinuxConfig.pm** ubicado en */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para establecer el valor del parámetro **SCSI_HOSTS_OPTIMIZED_RESCAN** en 1 para volver a analizar sólo los HBA que aparecen en HBA_DRIVER_NAMES.<br><br>• LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI<br>• VMDK en almacenes de datos VMFS o NFS<br>• Volúmenes NFS conectados directamente con el Guest VM |

### Tipos de almacenamiento compatibles con AIX

En la siguiente tabla se enumeran los tipos de almacenamiento admitidos en AIX.

| Máquina | Tipo de almacenamiento |
| --- | --- |
| Servidor físico | • LUN conectados a FC e iSCSI.<br><br>En un entorno SAN, se admiten los sistemas de archivos ASM, LVM y SAN.<br><br>No se admite NFS en AIX y sistema de archivos.<br><br>• Sistema de archivos con diario mejorado (JFS2)<br><br>Admite el registro en línea en sistemas DE archivos SAN y el diseño de LVM. |

La "Herramienta de matriz de interoperabilidad de NetApp" contiene la información más reciente acerca de las versiones con puerto.

## Privilegios mínimos requeridos de ONTAP para el plugin para Oracle

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

| **Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores** |
| --- |
| • event generate-autosupport-log |
| • se muestra el historial del trabajo<br>• detención de trabajo |

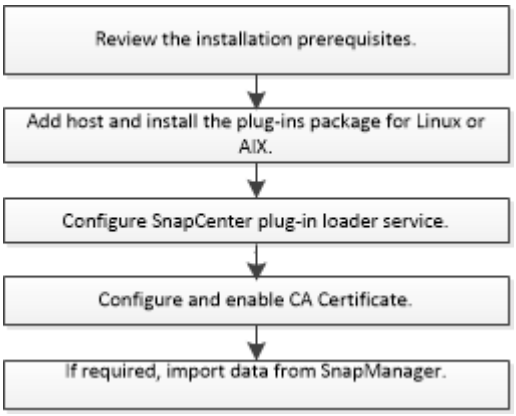
| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| • lun<br>• se muestra el atributo de lun<br>• lun create<br>• eliminación de lun<br>• geometría de lun<br>• igroup de lun añadido<br>• crear lun igroup<br>• lun igroup eliminado<br>• cambio de nombre de lun igroup<br>• lun igroup show<br>• asignación de lun de nodos adicionales<br>• se crea la asignación de lun<br>• se elimina la asignación de lun<br>• asignación de lun quitar nodos de generación de informes<br>• se muestra el mapa de lun<br>• modificación de lun<br>• movimiento de lun en volumen<br>• lun desconectada<br>• lun conectada<br>• reserva persistente de lun clara<br>• cambio de tamaño de lun<br>• serie de lun<br>• muestra de lun |
| • regla adicional de la política de snapmirror<br>• regla de modificación de la política de snapmirror<br>• regla de eliminación de la política de snapmirror<br>• la política de snapmirror<br>• restauración de snapmirror<br>• de snapmirror<br>• historial de snapmirror<br>• actualización de snapmirror<br>• conjunto de actualizaciones de snapmirror<br>• destinos de listas de snapmirror |
| • versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| • crear el clon de volumen<br>• show de clon de volumen<br>• inicio de división de clon de volumen<br>• detención de división de clon de volumen<br>• cree el volumen<br>• destrucción del volumen<br>• crear el archivo de volumen<br>• uso show-disk del archivo de volumen<br>• volumen sin conexión<br>• volumen en línea<br>• modificación del volumen<br>• crear el qtree de volúmenes<br>• eliminación de qtree de volumen<br>• modificación del qtree del volumen<br>• se muestra volume qtree<br>• restricción de volumen<br>• visualización de volumen<br>• crear snapshots de volumen<br>• eliminación de snapshots de volumen<br>• modificación de las copias de snapshot de volumen<br>• cambio de nombre de copias de snapshot de volumen<br>• restauración de copias snapshot de volumen<br>• archivo de restauración de snapshots de volumen<br>• visualización de copias de snapshot de volumen<br>• desmonte el volumen |
| • vserver<br>• vserver cifs<br>• se muestra vserver shadowcopy<br>• se muestra vserver |
| • interfaz de red<br>• se muestra la interfaz de red |
| • MetroCluster show |

# Instale el plugin de SnapCenter para base de datos de Oracle

## Flujo de trabajo de instalación del plugin de SnapCenter para base de datos de Oracle

Debe instalar y configurar el plugin de SnapCenter para base de datos de Oracle si desea proteger las bases de datos Oracle.




## Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux o AIX

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.

  El plugin de SnapCenter para base de datos Oracle puede ser instalado por un usuario no raíz. Sin embargo, debe configurar los privilegios sudo para el usuario no raíz para instalar e iniciar el proceso del plugin. Después de instalar el plugin, los procesos se ejecutan como un usuario raíz eficaz.

- Si va a instalar el paquete de plugins de SnapCenter para AIX en el host AIX, debe haber resuelto manualmente los enlaces simbólicos del nivel de directorio.

  El paquete de plugins de SnapCenter para AIX resuelve automáticamente el enlace simbólico del nivel de archivo, pero no los enlaces simbólicos del nivel de directorio para obtener la ruta absoluta DE JAVA_HOME.

- Cree credenciales con el modo de autenticación como Linux o AIX para el usuario de instalación.
- Debe haber instalado Java 1.8.x de 64 bits en el host Linux o AIX.

  Para obtener información sobre CÓMO descargar JAVA, consulte:

  - "Descargas de Java para todos los sistemas operativos"
  - "IBM Java para AIX"

- Para bases de datos Oracle que se ejecuten en un host Linux o AIX, debe instalar tanto el plugin de SnapCenter para base de datos Oracle como el plugin de SnapCenter para UNIX.

También es posible utilizar el plugin para bases de datos de Oracle para gestionar bases de datos de Oracle para SAP. Sin embargo, no se admite la integración con BR*Tools de SAP.

- Si utiliza la base de datos Oracle 11.2.0.3 o posterior, debe instalar la revisión 13366202 de Oracle.

### Requisitos del host Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de plugins de SnapCenter para Linux.

| Elemento | Requisitos |
|---|---|
| Sistemas operativos | • Red Hat Enterprise Linux<br>• Oracle Linux<br>Si utiliza la base de datos de Oracle en LVM en sistemas operativos Oracle Linux o Red Hat Enterprise Linux 6.6 o 7.0, tiene que instalar la versión más reciente del administrador de volúmenes lógicos (LVM).<br>• SUSE Linux Enterprise Server (SLES) |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 2 GB<br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |
| Paquetes de software obligatorios | Tipos Java 1.8.x (64 bits)Oracle Java y OpenJDK<br>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta. |

Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de

interoperabilidad de NetApp".

#### Configure privilegios sudo para usuarios que no son raíz para el host Linux

SnapCenter 2.0 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para Linux e inicie el proceso del plugin. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

### Lo que necesitará

- Sudo 1.8.7 o posterior.
- Asegúrese de que el usuario que no sea raíz forma parte del grupo de instalación de Oracle.
- Edite el archivo */etc/ssh/sshd_config* para configurar los algoritmos de código de autenticación de mensajes: Macs hmac-sha2-256 y MACs hmac-sha2-512.

  Reinicie el servicio sshd después de actualizar el archivo de configuración.

  Ejemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

### Acerca de esta tarea

Tiene que configurar los privilegios sudo para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- /Home/*SUDO_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl
- Pasos*

  1. Inicie sesión en el host Linux en el que desee instalar el paquete de plugins de SnapCenter para Linux.
  2. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux.

```
Cmnd_Alias SCCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/Linux_Prechecks.sh
SUDO_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: SUDO_USER env_keep=JAVA_HOME
Defaults: SUDO_USER !visiblepw
Defaults: SUDO_USER !requiretty
```

*SUDO_USER* es el nombre del usuario no raíz que ha creado.

Puede obtener el valor de suma de comprobación en el archivo **oracle_checksum.txt**, que se encuentra en *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Si ha especificado una ubicación personalizada, esta será *custom_path\NetApp\SnapCenter\Package Repository*.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

**Mejor práctica:** por razones de seguridad, debe eliminar la entrada sudo después de completar cada instalación o actualización.

### Requisitos del host AIX

Debe asegurarse de que el host cumpla los requisitos antes de instalar el paquete de plugins de SnapCenter para AIX.

El plugin de SnapCenter para UNIX que forma parte del paquete de plugins de SnapCenter para AIX, no admite grupos de volúmenes concurrentes.

| Elemento | Requisitos |
|---|---|
| Sistemas operativos | AIX 6.1 o posterior |
| RAM mínima para el plugin de SnapCenter en el host | 4 GB |

| Elemento | Requisitos |
| --- | --- |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 1 GB<br><br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |
| Paquetes de software obligatorios | Java 1.8.x (64 bits)IBM Java<br><br>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta. |

Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

#### Configure privilegios sudo para usuarios que no son raíz para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para AIX e inicie el proceso del plugin. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

**Lo que necesitará**

- Sudo 1.8.7 o posterior.
- Asegúrese de que el usuario que no sea raíz forma parte del grupo de instalación de Oracle.
- Edite el archivo */etc/ssh/sshd_config* para configurar los algoritmos de código de autenticación de mensajes: Macs hmac-sha2-256 y MACs hmac-sha2-512.

  Reinicie el servicio sshd después de actualizar el archivo de configuración.

  Ejemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

**Acerca de esta tarea**

Tiene que configurar los privilegios sudo para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl
- Pasos*

1. Inicie sesión en el host AIX en el que desee instalar el paquete de plugins de SnapCenter para AIX.
2. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux.

```
Cmnd_Alias SCCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
AIX_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

*AIX_USER* es el nombre del usuario que no es raíz que ha creado.

Puede obtener el valor de suma de comprobación en el archivo **oracle_checksum.txt**, que se encuentra en *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Si ha especificado una ubicación personalizada, esta será *custom_path\NetApp\SnapCenter\Package Repository*.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

**Mejor práctica:** por razones de seguridad, debe eliminar la entrada sudo después de completar cada instalación o actualización.

### Configure las credenciales

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar el paquete de plugins en hosts Linux o AIX.

### Acerca de esta tarea

Las credenciales se crean para el usuario raíz o para un usuario que no es raíz que tiene privilegios sudo para instalar e iniciar el proceso del plugin.

Para obtener más información, consulte: Configure privilegios sudo para usuarios que no son raíz para el host Linux o. Configure privilegios sudo para usuarios que no son raíz para el host AIX

**Práctica recomendada:** aunque se le permite crear credenciales después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Settings, haga clic en **Credential**.
3. Haga clic en **Nuevo**.
4. En la página Credential, introduzca la información de la credencial:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de credencial | Introduzca un nombre para las credenciales. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario/Contraseña | Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.<br>• Administrador del dominio<br>Especifique el administrador de dominio en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:<br>◦ *NetBIOS\Username*<br>◦ *Domain FQDN\Username*<br>• Administrador local (sólo para grupos de trabajo)<br>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: *Username* |
| Modo de autenticación | Seleccione el modo de autenticación que desea utilizar.<br>Según el sistema operativo del host del plugin, seleccione Linux o AIX. |
| Use privilegios sudo | Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz. |

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede que desee asignar mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

### Configurar credenciales para una base de datos Oracle

Es necesario configurar las credenciales que se usan para realizar operaciones de protección de datos en bases de datos de Oracle.

### Acerca de esta tarea

Debe revisar los diferentes métodos de autenticación compatibles con las bases de datos de Oracle. Para

obtener más información, consulte"Métodos de autenticación para las credenciales".

Si se configuran credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, el nombre de usuario debe tener al menos privilegios de grupo de recursos y backup.

Si habilitó la autenticación de base de datos de Oracle, se muestra un icono de candado rojo en la vista de recursos. Es necesario configurar las credenciales de la base de datos para poder proteger la base de datos, o bien añadirla al grupo de recursos para realizar operaciones de protección de datos.

Si especifica detalles incorrectos al crear una credencial, se muestra un mensaje de error. Debe hacer clic en **Cancelar** y luego volver a intentarlo.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** en la lista **View**.
3. Haga clic en y, a continuación, seleccione el nombre de host y el tipo de base de datos para filtrar los recursos.

   A continuación, puede hacer clic en para cerrar el panel de filtros.

4. Seleccione la base de datos y, a continuación, haga clic en **Configuración de base de datos** > **Configurar base de datos**.
5. En la sección Configure database settings, en la lista desplegable **Use existing Credential**, seleccione la credencial que debe utilizarse para realizar trabajos de protección de datos en la base de datos Oracle.

   El usuario de Oracle debe tener privilegios sysdba.

   También se puede crear una credencial si se hace clic en .

6. En la sección Configure ASM settings, en la lista desplegable **Use existing Credential**, seleccione la credencial que debe utilizarse para realizar trabajos de protección de datos en la instancia de ASM.

   El usuario de ASM debe tener privilegios sysasm.

   También se puede crear una credencial si se hace clic en .

7. En la sección Configurar los ajustes del catálogo RMAN, en la lista desplegable **utilizar credencial existente**, seleccione la credencial que debe utilizarse para realizar trabajos de protección de datos en la base de datos del catálogo de Oracle Recovery Manager (RMAN).

   También se puede crear una credencial si se hace clic en .

   En el campo **TNSName**, introduzca el nombre de archivo de sustrato de red transparente (TNS) que utilizará el servidor SnapCenter para comunicarse con la base de datos.

8. En el campo **nodos de RAC preferidos**, especifique los nodos de Real Application Cluster (RAC) preferidos para la copia de seguridad.

Estos nodos preferidos pueden ser uno o todos los nodos del clúster donde hay instancias de bases de datos de RAC presentes. La operación de backup se activa solo en estos nodos preferidos y en el orden indicado.

En RAC One Node, sólo un nodo aparece en los nodos preferidos y este nodo preferido es el nodo en el que la base de datos está alojada actualmente.

Después de la conmutación por error o la reubicación de la base de datos de RAC One Node, la actualización de recursos en la página Recursos de SnapCenter eliminará el host de la lista **nodos de RAC preferidos** donde se alojó la base de datos anteriormente. El nodo RAC en el que se reubica la base de datos aparecerá en **nodos RAC** y deberá configurarse manualmente como el nodo RAC preferido.

Para obtener más información, consulte "Nodos preferidos en la configuración de RAC".

1. Haga clic en **Aceptar**.

## Añada hosts e instale el paquete de plugins para Linux o AIX mediante la interfaz gráfica de usuario

Puede utilizar la página Add Host para añadir hosts y, a continuación, instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX. Los plugins se instalan automáticamente en hosts remotos.

### Acerca de esta tarea

Puede añadir un host e instalar paquetes de plugins para un host individual o para un clúster. Si instala el plugin en un clúster (Oracle RAC), el plugin se instala en todos los nodos del clúster. Para Oracle RAC One Node, debe instalar el plugin en nodos activos y pasivos.

Debe asignarse a un rol que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de host | Seleccione **Linux** o **AIX** como tipo de host.<br><br>El servidor de SnapCenter añade el host y, a continuación, instala el plugin para base de datos de Oracle y el plugin para UNIX si los plugins no están todavía instalados en el host. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de host | Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.<br><br>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.<br><br>Puede introducir las direcciones IP o el FQDN de uno de los siguientes:<br><br>• Host independiente<br>• Cualquier nodo en el entorno de Oracle Real Application Clusters (RAC)<br><br>El nodo VIP o IP de exploración no es compatible<br><br>Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar el FQDN. |
| Credenciales | Seleccione el nombre de credencial que ha creado o cree nuevas credenciales.<br><br>Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales.<br><br>Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado.<br><br>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. |

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto.<br><br>El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. |
| Ruta de instalación | La ruta predeterminada es */opt/NetApp/snapcenter*.<br><br>Opcionalmente, puede personalizar la ruta. |
| Añada todos los hosts en Oracle RAC | Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un Oracle RAC.<br><br>En una configuración de Flex ASM, se agregarán todos los nodos, independientemente de si se trata de un nodo Hub o Leaf. |
| Omitir comprobaciones previas a la instalación | Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin. |

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin.

   La secuencia de comandos comprobaciones previas no valida el estado del firewall del puerto del plugin si se especifica en las reglas de rechazo del firewall.

   Si no se cumplen los requisitos mínimos, se muestran los mensajes de error o advertencia pertinentes. Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en *C:\Program Files\NetApp\SnapCenter WebApp* para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero tendrá que solucionar el problema.

   En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Compruebe la huella y, a continuación, haga clic en **Confirmar y enviar**.

   En una configuración de clúster, debe comprobar la huella de cada uno de los nodos del clúster.

   SnapCenter no admite el algoritmo ECDSA.

   La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

1. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación están en */custom_location/snapcenter/logs*.

**Después de terminar**

Todas las bases de datos en el host se detectan automáticamente y se muestran en la página Resources. Si no aparece nada, haga clic en **Actualizar recursos**.

**Instale en varios hosts remotos mediante cmdlets**

Debe utilizar el cmdlet de PowerShell *Install-SmHostPackage* para instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX en varios hosts.

**Lo que necesitará**

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador en cada host en el que desee instalar el paquete de plugins.

- Pasos*

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet _Open-SmConnection y, a continuación, introduzca sus credenciales.
3. Instale el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX mediante el cmdlet *Install-SmHostPackage* y los parámetros necesarios.

   Puede utilizar la opción *-skipprecheck* cuando ya haya instalado los plugins manualmente y no desee validar si el host cumple los requisitos para instalar el plugin.

   La secuencia de comandos comprobaciones previas no valida el estado del firewall del puerto del plugin si se especifica en las reglas de rechazo del firewall.

1. Introduzca sus credenciales para la instalación remota.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

**Instale el paquete de plugins para Linux de forma interactiva**

Puede instalar el paquete de plugins de SnapCenter para Linux de forma interactiva en un host Linux.

**Lo que necesitará**

- Debe revisar los requisitos previos para instalar el paquete de plugins.
- Debe configurar la variable de entorno DISPLAY para especificar la dirección IP y el número de puerto del host Linux en el que desea iniciar el asistente.
- Pasos*
  1. Descargue el paquete de plugins de SnapCenter para Linux desde la ubicación de instalación del servidor SnapCenter.

     La ruta de instalación predeterminada es *C:\ProgramData\NetApp\SnapCenter\Package Repository*. Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

  2. Copie el archivo de instalación en el host en el que desea instalar el plugin.
  3. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación y ejecutado:
     `./SnapCenter_linux_host_plugin.bin –i swing`
  4. Siga las instrucciones que muestra el asistente para instalar el paquete de plugins.
  5. Haga clic en **Finalizar** para completar la instalación.

**Instale en el host del clúster**

Debe instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX en los dos nodos del host del clúster.

Cada uno de los nodos del host del clúster tiene dos IP. Una de las IP será la IP pública de los nodos correspondientes y la segunda IP será la IP de clúster que se compartirá entre ambos nodos.

- Pasos*
  1. Instale el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX en los dos nodos del host del clúster.
  2. Valide que los valores correctos de los parámetros SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT y SPL_ENABLED_PLUGINS se especifiquen en el archivo spl.properties ubicado en */var/opt/snapcenter/spl/etc/*.

     Si SPL_ENABLED_PLUGINS no se especifica en spl.properties, puede agregarla y asignar el valor SCO,SCU.

  3. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet _Open-SmConnection y, a continuación, introduzca sus credenciales.
  4. En cada uno de los nodos, establezca las IP preferidas del nodo mediante el comando *Set-PreferredHostIPsInStorageExportPolicy* sccli y los parámetros requeridos.
  5. En el host del servidor SnapCenter, agregue una entrada para la IP del clúster y el nombre DNS correspondiente en *C:\Windows\System32\drivers\etc\hosts*.
  6. Añada el nodo al servidor SnapCenter mediante el cmdlet *Add-SmHost* especificando la IP del clúster para el nombre de host.

Descubra la base de datos Oracle en el nodo 1 (suponiendo que la IP del clúster esté alojada en el nodo 1) y cree una copia de seguridad de la base de datos. Si se produce una conmutación por error, puede usar la copia de seguridad creada en el nodo 1 para restaurar la base de datos en el nodo 2. También puede usar el backup creado en el nodo 1 para crear un clon en el nodo 2.

Habrá volúmenes, directorios y archivos de bloqueo obsoletos si se produce la conmutación por error mientras se ejecuta cualquier otra operación de SnapCenter.

### Instale el paquete de plugins para Linux en modo silencioso o modo de consola

Puede instalar el paquete de plugins de SnapCenter para Linux en el modo consola o en el modo silencioso mediante la interfaz de la línea de comandos (CLI).

#### Lo que necesitará

- Debe revisar los requisitos previos para instalar el paquete de plugins.
- Debe asegurarse de que la variable de entorno DISPLAY no esté configurada.

  Si se establece la variable de entorno DISPLAY, se debe ejecutar unset DISPLAY y, a continuación, intentar instalar manualmente el plugin.

#### Acerca de esta tarea

Debe proporcionar la información de instalación necesaria mientras instala en el modo consola, mientras que en la instalación en modo silencioso no tiene que proporcionar ninguna información de instalación.

- Pasos*
  1. Descargue el paquete de plugins de SnapCenter para Linux desde la ubicación de instalación del servidor SnapCenter.

     La ruta de instalación predeterminada es *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

  2. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación.
  3. En función del modo de instalación que prefiera, lleve a cabo uno de los pasos siguientes.

| Modo de instalación | Pasos |
| --- | --- |
| Modo de consola | a. Ejecución:<br><br>`./SnapCenter_linux_host_plugin.bin -i console`<br><br>b. Siga las instrucciones en pantalla para completar la instalación. |
| Modo silencioso | Ejecución:<br><br>`./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-DUSER_INSTALL_DIR==/opt/custom_path` |

4. Edite el archivo spl.properties ubicado en */var/opt/snapcenter/spl/etc/* para añadir SPL_ENABLED_PLUGINS=SCO,SCU y, a continuación, reinicie el servicio de cargador de plugins de SnapCenter.

> La instalación del paquete de plugins registra los plugins en el host y no en SnapCenter Server. Para registrar los plugins de SnapCenter Server, debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Al añadir el host, seleccione “Ninguno” como credencial. Una vez añadido el host, los plugins instalados se detectan de forma automática.

### Instale el paquete de plugins para AIX en modo silencioso

Puede instalar el paquete de plugins de SnapCenter para AIX en modo silencioso mediante la interfaz de línea de comandos (CLI).

### Lo que necesitará

- Debe revisar los requisitos previos para instalar el paquete de plugins.
- Debe asegurarse de que la variable de entorno DISPLAY no esté configurada.

  Si se establece la variable de entorno DISPLAY, se debe ejecutar unset DISPLAY y, a continuación, intentar instalar manualmente el plugin.

- Pasos*
  1. Descargue el paquete de plugins de SnapCenter para AIX desde la ubicación de instalación del servidor SnapCenter.

     La ruta de instalación predeterminada es *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

  2. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación.
  3. Ejecución

     ```
     ./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
     DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
     DUSER_INSTALL_DIR==/opt/custom_path-
     DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
     DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
     ```

  4. Edite el archivo spl.properties ubicado en */var/opt/snapcenter/spl/etc/* para añadir SPL_ENABLED_PLUGINS=SCO,SCU y, a continuación, reinicie el servicio de cargador de plugins de SnapCenter.

> La instalación del paquete de plugins registra los plugins en el host y no en SnapCenter Server. Para registrar los plugins de SnapCenter Server, debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Al añadir el host, seleccione “Ninguno” como credencial. Una vez añadido el host, los plugins instalados se detectan de forma automática.

### Supervise el estado de la instalación

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de instalación.
     e. Haga clic en **aplicar**.
  4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configure el servicio de cargador de plugins de SnapCenter

El servicio de cargador de plugins de SnapCenter carga el paquete del plugin para Linux o AIX para interactuar con el servidor SnapCenter. El servicio de cargador de plugins de SnapCenter se instala cuando lo hace el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX.

### Acerca de esta tarea

Después de instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX, el servicio de cargador de plugins de SnapCenter se inicia de forma automática. Si el servicio de cargador de plugins de SnapCenter no se inicia de forma automática, tendrá que:

- Asegúrese de que no se haya eliminado el directorio donde está funcionando el plugin
- Aumente el espacio de la memoria asignado a la máquina virtual Java

El archivo spl.properties, que se encuentra en */custom_location/NetApp/snapcenter/spl/etc/*, contiene los

parámetros siguientes. Los valores predeterminados se asignan a estos parámetros.

| Nombre del parámetro | Descripción |
|---|---|
| NIVEL_REGISTRO | Muestra los niveles de los registros que se admiten.<br><br>Los posibles valores son INFO, DEBUG, TRACE, ERROR, FATAL, Y ADVIERTA. |
| SPL_PROTOCOL | Muestra el protocolo que admite el cargador del plugin de SnapCenter.<br><br>Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado. |
| SNAPCENTER_SERVER_PROTOCOL | Muestra el protocolo compatible con SnapCenter Server.<br><br>Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado. |
| SKIP_JAVAHOME_UPDATE | De forma predeterminada, el servicio SPL detecta la ruta de Java y el parámetro update JAVA_HOME.<br><br>Por lo tanto, el valor predeterminado se establece en FALSE. Puede establecer EN TRUE si desea deshabilitar el comportamiento predeterminado y corregir manualmente la ruta de acceso java. |
| SPL_KEYSTORE_PASS | Muestra la contraseña del archivo keystore.<br><br>Puede cambiar este valor solo si cambia la contraseña o crea un nuevo archivo keystore. |
| SPL_PORT | Muestra el número de puerto en el que se está ejecutando el cargador del plugin de SnapCenter.<br><br>Puede agregar el valor si falta el valor predeterminado.<br><br>No debe cambiar el valor después de instalar los plugins. |
| SNAPCENTER_SERVER_HOST | Muestra la dirección IP o el nombre de host del servidor SnapCenter. |
| SPL_KEYSTORE_RUTA | Muestra la ruta absoluta del archivo keystore. |
| SNAPCENTER_SERVER_PORT | Muestra el número de puerto en el que se está ejecutando el servidor SnapCenter. |

| Nombre del parámetro | Descripción |
| --- | --- |
| LOGS_MAX_COUNT | Muestra el número de archivos de registro del cargador del plugin de SnapCenter que se conservan en la carpeta */custom_location/snapcenter/spl/logs*.<br><br>El valor predefinido se establece en 5000. Si la cantidad es superior al valor especificado, se conservan los 5000 últimos archivos modificados. La comprobación del número de archivos se realiza de forma automática cada 24 horas desde el momento en que se inicia el servicio de cargador de plugins de SnapCenter.<br><br>Si elimina manualmente el archivo spl.properties, el número de archivos que se desea conservar se establece en 9999. |
| JAVA_HOME | Muestra la ruta del directorio absoluto DE JAVA_HOME que se utiliza para iniciar el servicio SPL.<br><br>Esta ruta se determina durante la instalación y como parte del SPL de inicio. |
| LOG_MAX_SIZE | Muestra el tamaño máximo del archivo de registro de trabajos.<br><br>Una vez alcanzado el tamaño máximo, el archivo de registro se comprime y los registros se escriben en el nuevo archivo de ese trabajo. |
| RETAIN_LOGS_OF_LAST_DAYS | Muestra el número de días hasta los que se conservan los registros. |
| ENABLE_CERTIFICATE_VALIDATION | Muestra TRUE cuando la validación de certificados de CA está habilitada para el host.<br><br>Puede habilitar o deshabilitar este parámetro editando la versión spl.properties o bien mediante la interfaz gráfica de usuario o el cmdlet de SnapCenter. |

Si cualquiera de estos parámetros no se asignan al valor predeterminado, o si desea asignar o cambiar el valor, puede modificar el archivo spl.properties. También puede verificar el archivo spl.properties y editarlo para solucionar los problemas relacionados con los valores que se asignan a los parámetros. Después de modificar el archivo spl.properties, tendrá que reiniciar el servicio de cargador de plugins de SnapCenter.

- Pasos*
  1. Ejecute una de las siguientes acciones, según sea necesario:

- Inicie el servicio de cargador de plugins de SnapCenter como usuario raíz:

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl start`
** Detenga el servicio de cargador de plugins de SnapCenter:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```

> Puede utilizar la opción -force con el comando stop para detener el servicio de cargador de plugins de SnapCenter enérgicamente. Sin embargo, debe ser cauteloso antes de hacerlo, ya que también termina las operaciones existentes.

- Reinicie el servicio de cargador de plugins de SnapCenter:

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
** Busque el estado del servicio de cargador de plugins de
SnapCenter:
```

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl status`
** Busque el cambio en el servicio de cargador de plugins de
SnapCenter:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

## Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux

Debe gestionar la contraseña del almacén de claves de SPL y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de SPL y configurar la pareja de claves firmadas de CA para el almacén de confianza de SPL con el servicio de cargador de plugins de SnapCenter para activar el certificado digital instalado.

> SPL utiliza el archivo 'keystore.jks', que se encuentra en ‘/var/opt/snapcenter/spl/etc’ tanto como su almacén de confianza como su almacén de claves.

### Gestione la contraseña para el almacén de claves SPL y el alias de la pareja de claves firmada de CA en uso

- Pasos*

1. Puede recuperar la contraseña predeterminada del almacén de claves del SPL desde el archivo de propiedades del SPL.

Es el valor correspondiente a la clave 'PL_KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

```
 keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña para todos los alias de las entradas de clave
privada en el almacén de claves por la misma contraseña utilizada
para el almacén de claves:
```

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

Actualice lo mismo para la clave SPL_KEYSTORE_PASS en el archivo spl.properties.1.

3. Reinicie el servicio después de cambiar la contraseña.

La contraseña para el almacén de claves SPL y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

**Configure los certificados intermedios o de raíz para el almacén de confianza SPL**

Debe configurar los certificados intermedios o de raíz sin la clave privada en el almacén de confianza de SPL.

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves SPL: */var/opt/snapcenter/spl/etc*.
  2. Busque el archivo 'keystore.jks'.
  3. Enumere los certificados añadidos al almacén de claves:

```
 keytool -list -v -keystore keystore.jks
. Añada un certificado raíz o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath>
-keystore keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza de SPL.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

**Configure la pareja de claves firmados de CA para el almacén de confianza SPL**

Debe configurar la pareja de claves firmada de CA en el almacén de confianza del SPL.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves /var/opt/snapcenter/spl/etc. de SPL
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
 keytool -list -v -keystore keystore.jks
. Agregue el certificado de CA con clave pública y privada.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Enumere los certificados añadidos al almacén de claves.
```

```
 keytool -list -v -keystore keystore.jks
. Compruebe que el almacén de claves contiene el alias
correspondiente al nuevo certificado de CA, que se añadió al almacén
de claves.
. Cambie la contraseña de clave privada añadida para el certificado
de CA a la contraseña del almacén de claves.
```

La contraseña predeterminada del almacén de claves SPL es el valor de la clave SPL_KEYSTORE_PASS en el archivo spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"
-keystore keystore.jks
. Si el nombre del alias del certificado de CA es largo y contiene
espacio o caracteres especiales ("*",","), cambie el nombre del alias
por un nombre simple:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure el nombre de alias del almacén de claves ubicado en el
archivo spl.propertiesI.
```

Actualice este valor contra la clave SPL_CERTIFICATE_ALIAS.

4. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza SPL.

**Configurar la lista de revocación de certificados (CRL) para SPL**

Debe configurar la CRL para SPL

**Acerca de esta tarea**

- SPL buscará los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de SPL es */var/opt/snapcenter/spl/etc/crl*.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo spl.properties con respecto a la CLAVE SPL_CRL_PATH.
  2. Puede colocar más de un archivo CRL en este directorio.

     Los certificados entrantes se verificarán en cada CRL.

## Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

### Lo que necesitará

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

### Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

# Importe datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter

Importar datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter le permite continuar usando sus datos de las versiones anteriores.

Puede importar datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter ejecutando la herramienta de importación desde la interfaz de línea de comandos (CLI de host Linux).

La herramienta de importación crea políticas y grupos de recursos en SnapCenter. Las políticas y los grupos de recursos creados en SnapCenter se corresponden con los perfiles y las operaciones realizadas mediante dichos perfiles en SnapManager para Oracle y SnapManager para SAP. La herramienta de importación de SnapCenter interactúa con las bases de datos del repositorio de SnapManager para Oracle y SnapManager para SAP, así como la base de datos que desee importar.

- Recupera todos los perfiles, las programaciones y las operaciones realizadas mediante los perfiles.
- Crea una política de backup de SnapCenter para cada operación única y cada programación adjunta a un perfil.
- Crea un grupo de recursos para cada base de datos de destino.

Puede ejecutar la herramienta de importación ejecutando el script sc-migrate ubicado en */opt/NetApp/snapcenter/spl/bin*. Al instalar el paquete de plugins de SnapCenter para Linux en el host de la base de datos que desea importar, el script sc-migrate se copia en */opt/NetApp/snapcenter/spl/bin*.

No es posible importar datos desde la interfaz gráfica de usuario (GUI) de SnapCenter.

SnapCenter no es compatible con Data ONTAP operando en 7-Mode. Puede utilizar la 7-Mode Transition Tool para migrar datos y configuraciones que se almacenan en un sistema que ejecuta Data ONTAP operando en 7-Mode a un sistema ONTAP.

### Configuraciones compatibles para la importación de datos

Antes de importar datos desde SnapManager 3.4.x para Oracle y SnapManager 3.4.x para SAP hacia SnapCenter, debe tener en cuenta cuáles son las configuraciones compatibles con el plugin de SnapCenter para base de datos de Oracle.

Las configuraciones compatibles con el plugin de SnapCenter para base de datos de Oracle se enumeran en la "Herramienta de matriz de interoperabilidad de NetApp".

### Qué elementos se importan en SnapCenter

Es posible usar los perfiles para importar perfiles, programas y operaciones ejecutados.

| De SnapManager para Oracle y SnapManager para SAP | A SnapCenter |
|---|---|
| Perfiles sin operaciones ni programas | Se crea una política con las opciones de tipo de backup Online y de alcance de backup Full. |

| De SnapManager para Oracle y SnapManager para SAP | A SnapCenter |
| --- | --- |
| Perfiles con una o más operaciones | Se crean múltiples políticas de acuerdo con una combinación única de un perfil y las operaciones ejecutadas por medio de ese perfil.<br><br>Las políticas que se crean en SnapCenter contienen los detalles de retención y de eliminación de registros de archivo que se recuperan del perfil y de las operaciones correspondientes. |
| Configurar perfiles con Oracle Recovery Manager (RMAN) | Las directivas se crean con la opción **Catalog backup with Oracle Recovery Manager** activada.<br><br>Si se utilizó la catalogación externa de RMAN en SnapManager, debe configurar los ajustes del catálogo de RMAN en SnapCenter. Puede seleccionar la credencial existente o crear una nueva credencial.<br><br>Si se configuró RMAN a través del archivo de control en SnapManager, no será necesario configurar RMAN en SnapCenter. |
| Programa conectado a un perfil | Se crea una política específica y exclusiva para el programa. |
| Base de datos | Se crea un grupo de recursos para cada base de datos que se importa.<br><br>En una configuración de Real Application Clusters (RAC), el nodo en el que se ejecuta la herramienta de importación se convierte en el nodo preferido tras la importación y se crea el grupo de recursos para ese nodo. |

Cuando se importa un perfil, se crea una política de verificación junto con la política de backups.

Si se importan en SnapCenter los perfiles, las programaciones y cualquier operación de SnapManager para Oracle y SnapManager para SAP, también se importan los distintos valores de los parámetros.

| Parámetros y valores de SnapManager para Oracle y SnapManager para SAP | Parámetros y valores de SnapCenter | Notas |
| --- | --- | --- |
| Alcance de backup<br>• Lleno<br>• SQL Server<br>• Registro | Alcance de backup<br>• Lleno<br>• SQL Server<br>• Registro | |
| Modo de backup<br>• Automático<br>• En línea<br>• Sin conexión | Tipo de backup<br>• En línea<br>• Apagado sin conexión | Si el modo de backup es Auto, la herramienta de importación verifica cuál era el estado de la base de datos cuando se ejecutó la operación y define, según corresponda, el tipo de backup como Online u Offline Shutdown. |
| Retención<br>• Días<br>• Recuentos | Retención<br>• Días<br>• Recuentos | SnapManager para Oracle y SnapManager para SAP utiliza tanto días como números para determinar la retención.<br>En SnapCenter, hay días *O* recuentos. Por lo tanto, la retención se define con respecto a los días, porque se prefieren los días antes que los números en SnapManager para Oracle y SnapManager para SAP. |
| Eliminar para programaciones<br>• Todo<br>• Número de cambio de sistema (SCN)<br>• Fecha<br>• Registros creados antes de horas, días, semanas y meses específicos | Eliminar para programaciones<br>• Todo<br>• Registros creados antes de horas y días específicos | SnapCenter no admite la eliminación basada en SCN, Fecha, semanas y meses. |

| Parámetros y valores de SnapManager para Oracle y SnapManager para SAP | Parámetros y valores de SnapCenter | Notas |
| --- | --- | --- |
| Notificación<br>• Solo se envían mensajes de correo electrónico sobre operaciones desarrolladas correctamente<br>• Solo se envían mensajes de correo electrónico sobre operaciones con errores<br>• Se envían mensajes de correo electrónico sobre operaciones desarrolladas correctamente y operaciones con errores | Notificación<br>• Siempre<br>• En caso de fallo<br>• Advertencia<br>• Error | Las notificaciones por correo electrónico se importan.<br>Sin embargo, debe actualizar manualmente el servidor SMTP con la interfaz gráfica de usuario de SnapCenter. El asunto del correo electrónico está en blanco para que usted lo configure. |

### Qué elementos no se importan en SnapCenter

La herramienta de importación no importa todos los elementos en SnapCenter.

Los siguientes elementos no se pueden importar en SnapCenter:

- Metadatos de backups
- Backups parciales
- Backups relacionados con Virtual Storage Console (VSC) y asignación de dispositivos sin formato (RDM)
- Roles o cualquier tipo de credenciales disponibles en el repositorio de SnapManager para SAP y SnapManager para Oracle
- Datos relacionados con operaciones de verificación, restauración y clonado
- Eliminar para operaciones
- Detalles de replicación especificados en el perfil de SnapManager para Oracle y el perfil de SnapManager para SAP

  Después de la importación, debe editar manualmente la política correspondiente creada en SnapCenter para incluir los detalles de la replicación.

- Información de backups catalogados

### Prepare la importación de datos

Antes de importar datos en SnapCenter, debe ejecutar determinadas tareas para ejecutar la operación de importación con éxito.

- Pasos*

  1. Identifique la base de datos que desea importar.
  2. Utilice SnapCenter para añadir el host de la base de datos e instalar el paquete de plugins de SnapCenter para Linux.

3. Utilice SnapCenter para configurar las conexiones de las máquinas virtuales de almacenamiento (SVM) que utilizan las bases de datos en el host.
4. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
5. En la página Resources, asegúrese de que se determina y se muestra la base de datos que deba importarse.

   Cuando desee ejecutar la herramienta de importación, la base de datos deberá estar accesible o se producirá un error al crear el grupo de recursos.

Si la base de datos cuenta con credenciales configuradas, deberá crear la credencial correspondiente en SnapCenter, asignar la credencial a la base de datos y, después, ejecutar de nuevo el descubrimiento de la base de datos. Si la base de datos se encuentra en Automatic Storage Management (ASM), deberá crear credenciales para la instancia de ASM y asignar la credencial a la base de datos.

1. Asegúrese de que el usuario que ejecute la herramienta de importación tenga derechos suficientes para ejecutar SnapManager para Oracle o SnapManager para comandos de la CLI de SAP (como el comando de suspender programaciones) desde SnapManager para Oracle o SnapManager para el host de SAP.
2. Ejecute los siguientes comandos en el host de SnapManager para Oracle o SnapManager para SAP a fin de suspender las programaciones:
   a. Si desea suspender las programaciones en el host de SnapManager para Oracle, ejecute:
      - `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smo credential set -profile -name profile_name`

        Debe ejecutar el comando smo credential set para cada perfil del host.

   b. Si desea suspender las programaciones en el host de SnapManager para SAP, ejecute:
      - `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smsap credential set -profile -name profile_name`

        Debe ejecutar el comando smsap credential set para cada perfil del host.
3. Asegúrese de que se muestre un nombre de dominio completo (FQDN) del host de la base de datos cuando ejecute hostname -f

   Si no se muestra un FQDN, debe modificar /etc/hosts para indicar el FQDN del host.

### Importar datos

Puede importar datos ejecutando la herramienta de importación desde el host de la base de datos.

### Acerca de esta tarea

Las políticas de backup de SnapCenter que se crean después de importar tienen diferentes formatos de nomenclatura:

- Las políticas creadas para los perfiles sin operaciones ni programaciones tienen el formato SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED.

  Cuando no se realicen operaciones mediante un perfil, la política correspondiente se creará con el tipo de backup predeterminado como en línea y el ámbito del backup como completo.

- Las políticas creadas para los perfiles con una o más operaciones tienen el formato SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- Las políticas creadas para las programaciones adjuntas a los perfiles tienen el formato SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- Pasos*
  1. Inicie sesión en el host de la base de datos que desee importar.
  2. Ejecute la herramienta de importación ejecutando el script sc-migrate ubicado en */opt/NetApp/snapcenter/spl/bin*.
  3. Introduzca el nombre de usuario y la contraseña del servidor SnapCenter.

     Después de validar las credenciales, se establecerá una conexión con SnapCenter.

  4. Especifique los detalles de la base de datos del repositorio de SnapManager para Oracle o SnapManager para SAP.

     La base de datos del repositorio incluye las bases de datos que están disponibles en el host.

  5. Especifique los detalles de la base datos de destino.

     Si desea importar toda la base de datos en el host, especifique all.

  6. Si desea generar un registro del sistema o enviar mensajes ASUP por operaciones con errores, tendrá que habilitarlos ejecutando los comandos *Add-SmStorageConnection* o *Set-SmStorageConnection*.

> Si desea cancelar una operación de importación, ya sea al ejecutar la herramienta de importación o después de la importación, debe eliminar manualmente las políticas de SnapCenter, las credenciales y los grupos de recursos creados como parte de la operación de importación.

### Resultados

Las políticas de backup de SnapCenter se crean para perfiles, programaciones y operaciones realizadas mediante los perfiles. Los grupos de recursos también se crean para cada base de datos de destino.

Después de importar los datos correctamente, las programaciones asociadas con la base de datos importada se suspenden en SnapManager para Oracle y SnapManager para SAP.

Después de importar, tiene que gestionar la base de datos importada o el sistema de archivos usando SnapCenter.

Los registros de cada ejecución de la herramienta de importación se almacenan en el directorio */var/opt/snapcenter/spl/logs* con el nombre spl_migration_timestamp.log. Puede consultar este registro para revisar los errores de importación y solucionar sus problemas.

# Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

## Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

## Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

# Preparar la protección de bases de datos de Oracle

Antes de ejecutar una operación de protección de datos, como un backup, un clon o una restauración, debe definir una estrategia y configurar el entorno. También debe configurar SnapCenter Server para que use las tecnologías SnapMirror y SnapVault.

Para aprovechar las ventajas de las tecnologías SnapVault y SnapMirror, debe configurar e inicializar una relación de protección de datos entre el volumen de origen y el volumen de destino en el dispositivo de almacenamiento. Puede usar NetApp System Manager o la línea de comandos de la consola de almacenamiento para ejecutar estas tareas.

Antes de usar el plugin para base de datos de Oracle, el administrador de SnapCenter debe instalar y configurar el servidor de SnapCenter y llevar a cabo las tareas de los requisitos previos.

- Instalar y configurar SnapCenter Server. "Leer más"
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento. "Leer más"

SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada SVM registrada en SnapCenter con registro de SVM o de clúster debe ser única.

- Cree credenciales con el modo de autenticación como Linux o AIX para el usuario de instalación. "Leer más"
- Añada hosts, instale los plugins y detecte los recursos.
- Si va a utilizar SnapCenter Server para proteger las bases de datos de Oracle que residen en LUN o VMDK de VMware RDM, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter.
- Instale Java en el host Linux o AIX.

  Consulte "Requisitos del host Linux" o. "Requisitos del host AIX" si quiere más información.
- Debe configurar el tiempo de espera del firewall de la aplicación con un valor de 3 horas o más.
- Si tiene bases de datos de Oracle en entornos NFS, debe haber configurado al menos una LIF de datos NFS para almacenamiento principal o secundario a fin de realizar operaciones de montaje, clonado, verificación y restauración.
- Si tiene varias rutas de datos (LIF) o una configuración de dNFS, puede realizar lo siguiente mediante la CLI de SnapCenter en el host de la base de datos:
  - De forma predeterminada, todas las direcciones IP del host de la base de datos se añaden a la directiva de exportación de almacenamiento de NFS en la máquina virtual de almacenamiento (SVM) para los volúmenes clonados. Si desea contar con una dirección IP específica o restringir a una subred de direcciones IP, ejecute la CLI de Set-PreferredHostIPsInStorageExportPolicy.
  - Si tiene varias LIF en la SVM, SnapCenter elije la ruta de LIF correspondiente para montar el volumen clonado de NFS. No obstante, si desea especificar una determinada ruta de LIF, debe ejecutar la CLI de Set-SvmPreferredDataPath. La guía de referencia de comandos tiene más información.
- Si tiene bases de datos de Oracle en entornos SAN, asegúrese de que el entorno SAN esté configurado según las recomendaciones mencionadas en las siguientes guías:
  - "Configuración del host recomendada para Linux Unified Host Utilities"
  - "Uso de hosts Linux con almacenamiento de ONTAP"
  - "Configuración del host afectada por AIX Host Utilities"
- Si tiene bases de datos de Oracle en LVM en sistemas operativos Oracle Linux o RHEL, instale la versión más reciente de Logical Volume Management (LVM).
- Si utiliza SnapManager para Oracle y desea migrar al plugin de SnapCenter para base de datos de Oracle, puede migrar los perfiles a políticas y grupos de recursos de SnapCenter usando el comando sccli sc-Migrate.
- Configure SnapMirror y SnapVault en ONTAP si quiere realizar una replicación de backup

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para los usuarios de SnapCenter 4.3.x, la documentación del plugin de SnapCenter para VMware vSphere 4.3 tiene información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual del plugin de SnapCenter para VMware vSphere basado en Linux (formato de dispositivo virtual abierto).

**Más información**

- "Herramienta de matriz de interoperabilidad"

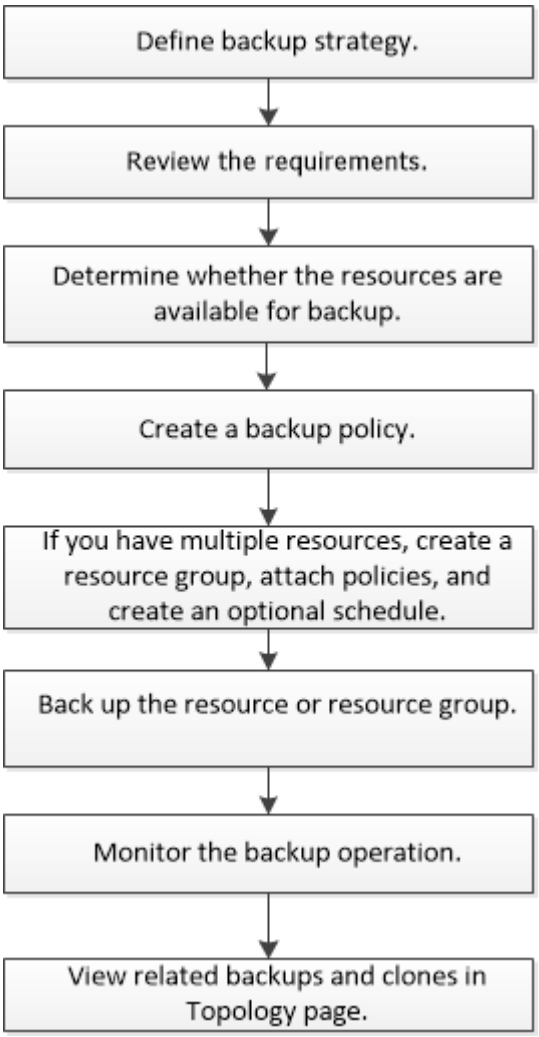
- "Documentación del plugin de SnapCenter para VMware vSphere"
- "Error en la operación de protección de datos en un entorno no multivía en RHEL 7 y versiones posteriores"

# Realice backups de bases de datos de Oracle

## Flujo de trabajo de backup

Es posible crear un backup de un recurso (base de datos) o un grupo de recursos. El flujo de trabajo de backup incluye planificación, identificación de los recursos para el backup, creación de políticas de backup, creación de grupos de recursos y vinculación de políticas, creación de backups y supervisión de las operaciones.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:




Al crear un backup para bases de datos de Oracle, se crea un archivo de bloqueo operativo (.sm_lock_dbsid) en el host de la base de datos de Oracle, en el directorio *$ORACLE_HOME/DBS*, para evitar que se ejecuten varias operaciones en la base de datos. Después de realizar el backup de la base de datos, se elimina automáticamente el archivo de bloqueo operativo.

Sin embargo, si la copia de seguridad anterior se completó con una advertencia, es posible que el archivo de bloqueo operativo no se elimine y la próxima operación de copia de seguridad entra en la cola de espera. Es posible que finalmente se cancele si el archivo **.sm_lock_dbsid** no se elimina. En este caso, debe eliminar manualmente el archivo de bloqueo operativo siguiendo estos pasos:

1. En la línea de comandos, desplácese hasta $ORACLE_HOME/DBS.
2. Elimine el bloqueo operativo:`rm -rf .sm_lock_dbsid.`

## Definir una estrategia de backup para bases de datos de Oracle

Definir una estrategia de backup antes de crear las tareas de backup garantiza que se cuente con todos los backups necesarios para restaurar o clonar correctamente las bases de datos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

#### Configuraciones de bases de datos de Oracle para backups admitidas

SnapCenter admite el backup de diferentes configuraciones de bases de datos de Oracle.

- Oracle independiente
- Real Application Clusters (RAC) de Oracle
- Oracle Standalone Legacy
- Base de datos de contenedores independiente de Oracle (CDB)
- Oracle Data Guard en espera

  Solo se pueden crear backups sin conexión montados de bases de datos en espera de Data Guard. No se admiten el backup sin conexión apagado, el backup de solo registro de archivos y el backup completo.

- Oracle Active Data Guard en espera

  Solo pueden crearse backups en línea de bases de datos en espera de Active Data Guard. No se admiten el backup solo de registro de archivo y el backup completo.

  > Antes de crear un backup de una base de datos en espera de Data Guard o Active Data Guard, se detiene el proceso de recuperación gestionado (MRP) y, una vez que se crea el backup, se inicia MRP.

- Gestión automática del almacenamiento (ASM)
  - ASM independiente y ASM RAC en disco de máquina virtual (VMDK)

    > Entre todos los métodos de restauración compatibles con las bases de datos de Oracle, solo se puede ejecutar la restauración por conexión y copia de bases de datos de ASM RAC en VMDK.

- ASM independiente y ASM RAC en asignación de dispositivos sin formato (RDM) es posible realizar operaciones de backup, restauración y clonado en bases de datos de Oracle en ASM, con o sin ASMLib.
- Controlador de filtro de Oracle ASM (ASMFD)

  No se admiten las operaciones de migración de PDB y clonado de PDB.

- Oracle Flex ASM

Para obtener la información más reciente sobre las versiones de Oracle admitidas, consulte "Herramienta de matriz de interoperabilidad de NetApp".

### Tipos de backup compatibles con las bases de datos de Oracle

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite los tipos backup en línea y sin conexión para bases de datos de Oracle.

#### Backup en línea

Un backup que se crea cuando la base de datos está en estado en línea se denomina backup en línea. También denominado backup dinámico, un backup en línea permite crear un backup de la base de datos sin apagarlo.

Como parte del backup en línea, es posible crear un backup de los siguientes archivos:

- Solo archivos de datos y archivos de control
- Solo archivos del registro de archivos (en este escenario, la base de datos no se coloca en modo de backup)
- Base de datos completa, que incluye archivos de datos, archivos de control y archivos del registro de archivos

#### Backup sin conexión

Un backup creado cuando la base de datos está en estado montado o apagado se denomina backup sin conexión. Este tipo de backup también se denomina backup en frío. Es posible incluir solo archivos de datos y archivos de control en los backups sin conexión. Puede crear un backup sin conexión montado o apagado sin conexión.

- Cuando se crea un backup sin conexión montado, la base de datos debe estar en estado montado.

  Si está en cualquier otro estado, la operación de backup generará errores.

- Al crear un backup sin conexión apagado, la base de datos puede estar en cualquier estado.

  El estado de la base de datos se modifica para alcanzar el estado deseado y poder crear el backup. Después de crear el backup, el estado de la base de datos se revierte a su estado original.

### Cómo detecta SnapCenter las bases de datos de Oracle

"Resources" son las bases de datos de Oracle en el host que mantiene SnapCenter. Es posible añadir estas bases de datos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos disponibles. Debe tener en cuenta el proceso que sigue SnapCenter para detectar diferentes tipos y versiones de las bases de datos de Oracle.

| Para las versiones de Oracle 11*g* a 12*c*R1 | Para las versiones de Oracle 12*c*R2 a 18*c*_ |
| --- | --- |
| **Base de datos RAC**: Las bases de datos RAC se detectan sólo sobre la base de entradas /etc/oratab.<br><br>Deben tener las entradas de la base de datos en el archivo /etc/oratab. | **Base de datos RAC**: Las bases de datos RAC se detectan con el comando srvctl config. |
| **Standalone**: Las bases de datos independientes se detectan sólo sobre la base de entradas /etc/oratab.<br><br>Deben tener las entradas de la base de datos en el archivo /etc/oratab. | **Standalone**: Las bases de datos independientes se detectan según las entradas del archivo /etc/oratab y la salida del comando srvctl config. |
| **ASM**: La entrada de instancia ASM debería estar disponible en el archivo /etc/oratab. | **ASM**: No es necesario que la entrada de instancia ASM esté en el archivo /etc/oratab. |

| Para las versiones de Oracle 11*g* a 12*c*R1 | Para las versiones de Oracle 12*c*R2 a 18*c*_ |
| --- | --- |
| **RAC One Node**: Las bases de datos RAC One Node se detectan sólo sobre la base de entradas /etc/oratab.<br><br>Las bases de datos deben estar en el estado *nomount*, *Mount* o *open*. Deben tener las entradas de la base de datos en el archivo /etc/oratab.<br><br>El estado de la base de datos de RAC One Node se marcará como cambiado de nombre o se eliminará si la base de datos ya se detecta y los backups se asocian a la base de datos.<br><br>Si se reubica la base de datos, debe realizar los siguientes pasos:<br><br>1. Añada manualmente la entrada de la base de datos reubicada en el archivo /etc/oratab en el nodo RAC con error.<br>2. Actualice manualmente los recursos.<br>3. Seleccione la base de datos RAC One Node de la página de recursos y, a continuación, haga clic en **Configuración de base de datos**.<br>4. Configure la base de datos para establecer los nodos de clúster preferidos en el nodo de RAC que aloja actualmente la base de datos.<br>5. Ejecute las operaciones de SnapCenter.<br><br>Si se recolocó una base de datos de un nodo a otro y si la entrada oratab del nodo anterior no se elimina, se debe eliminar manualmente la entrada oratab para evitar que la misma base de datos se muestre dos veces. | **RAC One Node**: Las bases de datos RAC One Node se detectan sólo con el comando srvctl config .<br><br>Las bases de datos deben estar en el estado *nomount*, *Mount* o *open*. El estado de la base de datos de RAC One Node se marcará como cambiado de nombre o se eliminará si la base de datos ya se detecta y los backups se asocian a la base de datos.<br><br>Si se reubica la base de datos, debe realizar los siguientes pasos:<br><br>1. Actualice manualmente los recursos.<br>2. Seleccione la base de datos RAC One Node en la página de recursos y, a continuación, haga clic en **Configuración de base de datos**.<br>3. Configure la base de datos para establecer los nodos de clúster preferidos en el nodo de RAC que aloja actualmente la base de datos.<br>4. Ejecute las operaciones de SnapCenter. |

Si hay alguna entrada de base de datos de Oracle 12*c*R2 y 18*c* en el archivo /etc/oratab y la misma base de datos se registra con el comando srvctl config, SnapCenter eliminará las entradas de base de datos duplicadas. Si hay entradas obsoletas de la base de datos, la base de datos se descubrirá, pero no se podrá acceder a la base de datos y el estado será sin conexión.

### Nodos preferidos en la configuración de RAC

En una configuración de Real Application Clusters (RAC) de Oracle, es posible especificar los nodos preferidos para ejecutar la operación de backup. Si no se especifica un nodo preferido, SnapCenter asigna automáticamente un nodo como preferido y lo usa para crear el backup.

Los nodos preferidos pueden ser uno o varios de los nodos del clúster donde se encuentran las instancias de la base de datos de RAC. La operación de backup se activa únicamente en esos nodos preferidos en el orden

de preferencia indicado.

Ejemplo: La base de datos de RAC cdbrac tiene tres instancias: Cdbrac1 en el nodo 1, cdbrac2 en el nodo 2 y cdbrac3 en el nodo 3. Las instancias 1 y 2 están configuradas como preferidos, con el nodo 2 en el primer lugar de preferencia y el nodo 1 en el segundo. Cuando se ejecuta una operación de backup, primero se intenta en el nodo 2, ya que es el primero en preferencia. Si el nodo 2 no tiene un estado adecuado para el backup, lo cual puede deberse a diversos motivos, por ejemplo, que el agente del plugin no esté en ejecución en el host, la instancia de la base de datos del host no tiene el estado requerido para el tipo de backup especificado, O la instancia de base de datos del nodo 2 en una configuración de FlexASM no sirve a la instancia de ASM local; luego se intenta ejecutar la operación en el nodo 1. El nodo 3 no se usará para el backup, ya que no es parte de la lista de nodos preferidos.

En una configuración de Flex ASM, los nodos de hoja no se mostrarán como nodos preferidos si la cardinalidad es inferior al número de nodos del clúster de RAC. Si hay algún cambio en las funciones del nodo del clúster de ASM de Flex, debe detectar manualmente para que se actualicen los nodos preferidos.

#### Estado de la base de datos necesario

Las instancias de base de datos de RAC de los nodos preferidos deben tener el estado necesario para que el backup se ejecute correctamente:

- Una de las instancias de base de datos de RAC de los nodos preferidos configurados debe tener el estado abierto para que se pueda crear un backup en línea.
- Una de las instancias de base de datos de RAC de los nodos preferidos configurados debe tener el estado de montaje y las demás instancias, incluidos los demás nodos preferidos, deben tener el estado de montaje o un valor inferior para crear un backup de montaje sin conexión.
- Las instancias de base de datos de RAC pueden tener cualquier estado, pero es necesario especificar los nodos preferidos para poder crear un backup de apagado sin conexión.

### Cómo catalogar backups con Oracle Recovery Manager

Es posible catalogar los backups de bases de datos de Oracle con Oracle RMAN para almacenar la información de backups en el repositorio de Oracle RMAN.

Posteriormente, se pueden utilizar los backups catalogados para operaciones de restauración a nivel de bloque o de recuperación de un momento específico en el espacio de tabla. Cuando no se necesitan estos backups catalogados, es posible quitar la información de catálogo.

La base de datos debe estar en un estado montado o superior para la catalogación. Es posible realizar la catalogación en backups de datos, backups de registros de archivo y backups completos. Si se habilita la catalogación para un backup de un grupo de recursos que contiene varias bases de datos, se realiza la catalogación en cada base de datos. Para las bases de datos de Oracle RAC, la catalogación se realiza en el nodo preferido donde la base de datos se encuentra al menos en estado montado.

> Si desea catalogar backups de una base de datos de RAC, asegúrese de que no exista otro trabajo en ejecución para esa base de datos. Si existe otro trabajo en ejecución, la operación de catalogación genera un error se interrumpe tras generar un error y no se colocar en cola.

De forma predeterminada, se utiliza el archivo de control de la base de datos de destino para la catalogación. Si desea añadir una base de datos de catálogo externo, puede especificar la credencial y el nombre de sustrato de red transparente (TNS) para el catálogo externo en el asistente Database Settings de la interfaz gráfica de usuario (GUI) de SnapCenter para configurar esa base de datos. También es posible ejecutar el comando Configure-SmOracleDatabase con las opciones -OracleRmanCatalogCredentialName y -OracleRmanCatalogTnsName para configurar la base de datos de catálogo externo desde la interfaz de línea

de comandos.

Si habilitó la opción de catalogación durante la creación de una política de backup de Oracle desde la interfaz gráfica de usuario de SnapCenter, los backups se catalogan mediante Oracle RMAN como parte de la operación de backup. También puede ejecutar el comando Catalog-SmBackupWithOracleRMAN para realizar una catalogación diferida de backups. Después de catalogar los backups, puede ejecutar el comando Get-SmBackupDetails para obtener la información de backups catalogados, como las ubicaciones de los registros de archivo, la etiqueta para los archivos de datos catalogados y la ruta de catálogo para el archivo de control.

Si el nombre del grupo de discos de ASM contiene 16 caracteres o más, en SnapCenter 3.0, el formato de nomenclatura que se utiliza para el backup es SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. Sin embargo, si el nombre del grupo de discos tiene menos de 16 caracteres, el formato de nomenclatura utilizado para la copia de seguridad es DISKGROUPNAME_DBSID_BACKUPID, que es el mismo formato utilizado en SnapCenter 2.0.

HASHCODEofDISKGROUP es un número generado automáticamente (de 2 a 10 dígitos) que es exclusivo de cada grupo de discos de ASM.

Es posible realizar verificaciones cruzadas para actualizar la información obsoleta en el repositorio de RMAN sobre los backups con registros de repositorio que no coinciden con su estado físico. Por ejemplo, si un usuario quita registros archivados del disco con un comando del sistema operativo, se seguirá indicando en el archivo de control que los registros están en el disco, cuando realmente no lo están. La operación de verificación cruzada permite actualizar el archivo de control con la información. Para habilitar la verificación cruzada, puede ejecutar el comando Set-SmConfigSettings y asignar el valor TRUE al parámetro ENABLE_CROSSCHECK. De forma predeterminada, el valor se establece en FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Para quitar la información de catálogo, puede ejecutar el comando Uncatalog-SmBackupWithOracleRMAN. No se puede quitar la información de catálogo mediante la interfaz gráfica de usuario de SnapCenter. Sin embargo, la información de un backup catalogado se quita mientras se elimina el backup o mientras se eliminan la retención y el grupo de recursos asociado a ese backup catalogado.

Cuando se fuerza la eliminación de un host de SnapCenter, no se quita la información de los backups catalogados asociados a ese host. Es necesario quitar la información de todos los backups catalogados de ese host para poder forzar la eliminación del host.

Si se produce un error de catalogación y descatalogación porque el tiempo de la operación superó el valor especificado de tiempo de espera en el parámetro ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT, debe modificar el valor del parámetro ejecutando el siguiente comando:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Después de modificar el valor del parámetro, reinicie SnapCenter el servicio del SPL con el siguiente comando:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help nombre_comando. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".

### Programaciones de backup

La frecuencia de los backups (tipo de programación) se especifica en las políticas; la programación de los backups se especifica en la configuración del grupo de recursos. El factor más crítico para determinar la frecuencia o la programación de los backups es la tasa de cambio del recurso y la importancia de los datos. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores son la importancia del recurso para la organización, el SLA y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso en el caso de un recurso utilizado intensivamente, no existe el requisito de ejecutar un backup completo más de una o dos veces al día. Por ejemplo, es posible que sea suficiente realizar backups regulares de registros de transacciones para garantizar los backups necesarios Cuanto mayor sea la frecuencia con que realiza backups de las bases de datos, menos registros de transacciones deberá utilizar SnapCenter en el momento de la restauración, lo que puede dar como resultado operaciones más rápidas.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de los backups (cada cuánto tiempo deben realizarse los backups), denominada *schedule type* para algunos plugins, forma parte de la configuración de una política. Se puede seleccionar una frecuencia de backups por hora, por día, por semana o por mes para la política. Si no selecciona ninguna de estas frecuencias, la política creada es de sólo bajo demanda. Puede acceder a las directivas haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

  Las programaciones de los backups (el momento exacto en que se realizan los backups) forman parte de una configuración de grupo de recursos. Por ejemplo, si tiene un grupo de recursos que posee una política configurada para backups semanales, quizás sea conveniente configurar la programación para que realice backups todos los jueves a las 00:10. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **grupos de recursos**.

### Convenciones de nomenclatura de backups

Es posible usar la convención de nomenclatura de copia Snapshot predeterminada o usar una convención de nomenclatura personalizada. La convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de las copias de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La copia Snapshot usa la siguiente convención de nomenclatura predeterminada:

```
resourcegroupname_hostname_timestamp
```

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre de host.
- *03-12-2015_23.17.26* es la fecha y la marca de hora.

Como alternativa, puede especificar el formato de nombre de la copia Snapshot mientras protege los recursos o grupos de recursos seleccionando **usar formato de nombre personalizado para copia Snapshot**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la copia de Snapshot.

#### Opciones de retención de backups

Es posible elegir la cantidad de días durante los cuales se retendrán las copias de backup o especificar la cantidad de copias de backup que se desean retener, con un máximo de 255 copias en ONTAP. Por ejemplo, una organización puede necesitar retener 10 días de copias de backup o 130 copias de backup.

Al crear una política, es posible especificar las opciones de retención para cada tipo y programación de backup.

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

SnapCenter elimina los backups previos que tengan etiquetas de retención que coincidan con el tipo de programación. Si se modifica el tipo de programación para el recurso o el grupo de recursos, los backups con la etiqueta del tipo de programación anterior podrían conservarse en el sistema.

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

#### Verifique la copia de backup con un volumen de almacenamiento primario o secundario

Es posible verificar las copias de backups en el volumen de almacenamiento principal o en el volumen de almacenamiento secundario de SnapMirror y SnapVault. La verificación con un volumen de almacenamiento secundario reduce la carga para el volumen de almacenamiento principal.

Cuando se verifica un backup que se encuentra en el volumen de almacenamiento primario o secundario, todas las copias de Snapshot primarias y secundarias se marcan como verificadas.

Se necesita una licencia de SnapRestore para verificar copias de backup en un volumen de almacenamiento secundario de SnapMirror o SnapVault.

## Determinar si las bases de datos de Oracle están disponibles para backup

Los recursos son bases de datos de Oracle en el host gestionado por SnapCenter. Es posible añadir estas bases de datos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos disponibles.

#### Lo que necesitará

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir credenciales.
- Si las bases de datos residen en un disco de máquina virtual (VMDK) o una asignación de dispositivo sin

formato (RDM), es necesario implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter.

Para obtener más información, consulte "Ponga en marcha el plugin de SnapCenter para VMware vSphere".

- Si las bases de datos residen en un sistema de archivos VMDK, debe haber iniciado sesión en vCenter y navegado hasta **VM options** > **Advanced** > **Edit Configuration** para configurar el valor de *disk.enableUUID* en true para la máquina virtual.
- Debe haber revisado el proceso que sigue SnapCenter para detectar diferentes tipos y versiones de las bases de datos de Oracle.

**Acerca de esta tarea**

Después de instalar el plugin, todas las bases de datos en ese host se detectan de forma automática y se muestran en la página Resources.

Las bases de datos deben estar en estado montado o superior para que la detección de la base de datos sea exitosa. En un entorno Oracle RAC, la instancia de la base de datos de RAC en el host donde se realiza la detección, debe estar en estado montado o superior para que la detección de la instancia de la base de datos sea exitosa. Solo las bases de datos que se detecten exitosamente pueden añadirse a los grupos de recursos.

Si eliminó una base de datos de Oracle en el host, el servidor de SnapCenter no tendrá conocimiento y enumerará la base de datos eliminada. Debe actualizar manualmente los recursos para actualizar la lista de recursos de SnapCenter.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Database** en la lista **View**.

     Haga clic en y, a continuación, seleccione el nombre de host y el tipo de base de datos para filtrar los recursos. A continuación, haga clic en el para cerrar el panel de filtros.

  3. Haga clic en **Actualizar recursos**.

     En un escenario de RAC One Node, la base de datos se detecta como la base de datos de RAC en el nodo en el que está alojado actualmente.

**Resultados**

Las bases de datos se muestran junto con información como el tipo de base de datos, el nombre del clúster o host, las políticas y los grupos de recursos asociados, y el estado.

- Si la base de datos está en un sistema de almacenamiento de terceros, la interfaz de usuario muestra el mensaje Not available for backup en la columna Overall Status.

  No es posible realizar operaciones de protección de datos en una base de datos que está en un sistema de almacenamiento de terceros.

- Si la base de datos está en un sistema de almacenamiento de NetApp y no está protegida, la interfaz de usuario muestra un mensaje Not protected en la columna Overall Status.
- Si la base de datos está en un sistema de almacenamiento de NetApp y está protegida, la interfaz de

usuario muestra un mensaje Available for backup en la columna Overall Status.

Si habilitó una autenticación de base de datos de Oracle, se muestra un icono de candado rojo en la vista de recursos. Es necesario configurar las credenciales de la base de datos para poder proteger la base de datos, o bien añadirla al grupo de recursos para realizar operaciones de protección de datos.

## Crear políticas de backup para bases de datos de Oracle

Antes de usar SnapCenter para realizar backups de recursos de base de datos de Oracle, debe crear una política de backup para el recurso o el grupo de recursos que se respaltendrá. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups. También puede especificar la configuración de replicación, script y tipo de backup. Crear una política permite ahorrar tiempo cuando se desea volver a utilizar esa política en otro recurso o grupo de recursos.

**Lo que necesitará**

- Debe tener definida una estrategia de backup.
- En el marco de los preparativos para la protección de datos, completó tareas como instalar SnapCenter, añadir hosts, detectar bases de datos y crear conexiones del sistema de almacenamiento.
- Si desea replicar copias de Snapshot en un almacenamiento secundario con SnapMirror o SnapVault, el administrador de SnapCenter debe haberle asignado las SVM de los volúmenes de origen y de destino.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Directivas**.
3. Seleccione **Oracle Database** en la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Name, escriba el nombre de la política y una descripción.
6. En la página Backup Type, realice los siguientes pasos:

    - Si desea **crear una copia de seguridad en línea**, seleccione **copia de seguridad en línea**.

      Debe especificar si desea realizar un backup de todos los archivos de datos, los archivos de control y los archivos de registro de archivos, solo de los archivos de datos y los archivos de control, o solo de los archivos de registro de archivos.

    - Si desea **crear una copia de seguridad sin conexión**, seleccione **copia de seguridad sin conexión** y, a continuación, seleccione una de las siguientes opciones:
        - Si desea crear una copia de seguridad sin conexión cuando la base de datos está en estado montado, seleccione **Mount**.
        - Si desea crear una copia de seguridad de apagado sin conexión cambiando el estado de la base de datos a apagado, seleccione **Apagar**.

          Si tiene bases de datos conectables (PDB) y desea guardar el estado de las PDB antes de crear el backup, debe seleccionar **Guardar estado de PDB**. Esto permite que las PDB regresen a su estado original después de la creación del backup.

- Especifique la frecuencia de programación seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

  Es posible especificar la programación (fecha de inicio y fecha de finalización) para la operación de backup mientras se crea un grupo de recursos. De este modo, puede crear grupos de recursos que compartan la misma política y la misma frecuencia de backup, pero también asignar diferentes programaciones de backup a cada política.

  Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

- Si desea catalogar la copia de seguridad con Oracle Recovery Manager (RMAN), seleccione **Catalog backup with Oracle Recovery Manager (RMAN)**.

  Puede realizar una catalogación diferida de un backup a la vez con la interfaz gráfica de usuario o con el comando Catalog-SmBackupWithOracleRMAN de la CLI de SnapCenter.

  Si desea catalogar backups de una base de datos de RAC, asegúrese de que no exista otro trabajo en ejecución para esa base de datos. Si existe otro trabajo en ejecución, la operación de catalogación genera un error se interrumpe tras generar un error y no se colocar en cola.

- Si desea reducir los registros de archivos después de la copia de seguridad, seleccione **Prune archive logs after backup**.

  Se omitirá la eliminación de registros de archivo desde el destino del registro de archivos que no esté configurado en la base de datos.

  Si está utilizando Oracle Standard Edition, puede utilizar los parámetros LOG_ARCHIVE_DEST y LOG_ARCHIVE_DUPLEX_DEST al realizar una copia de seguridad del registro de archivos.

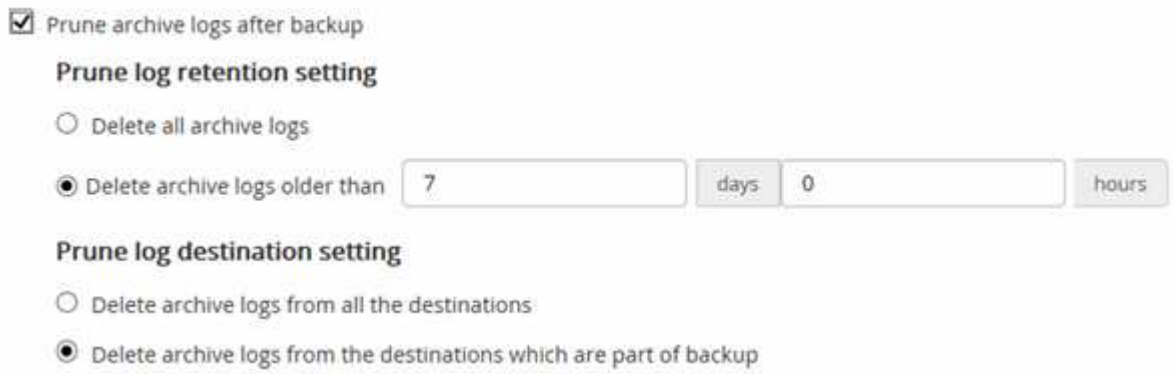
- Puede eliminar los registros de archivos únicamente si seleccionó los archivos de registro de archivos como parte del backup.

  Debe asegurarse de que todos los nodos en el entorno RAC puedan acceder a todas las ubicaciones del registro de archivos para que la operación de eliminación se complete correctamente.

| **Si desea…** | **Realice lo siguiente…** |
| --- | --- |
| Elimine todos los registros de archivos | Seleccione **Eliminar todos los registros de archivo**. |
| Elimine los registros de archivos antiguos | Seleccione **Eliminar registros de archivo de más de** y, a continuación, especifique la antigüedad de los registros de archivo que se eliminarán en días y horas. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Elimine los registros de archivos en todos los destinos | Seleccione **Eliminar registros de archivo de todos los destinos**. |
| Eliminar los registros de archivos de los destinos de registro que forman parte del backup | Seleccione **Eliminar registros de archivo de los destinos que forman parte de copia de seguridad**. |

+




7. En la página Retention, especifique la configuración de retención para el tipo de backup y el tipo de programación seleccionados en la página Backup Type:

| Si desea… | Realice lo siguiente… |
| --- | --- |

| | |
|---|---|
| Conservar una cierta cantidad de copias de Snapshot | Seleccione **total Snapshot copies to keep** y, a continuación, especifique el número de copias Snapshot que desea conservar.<br><br>Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas.<br><br>El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.<br><br>Debe establecer el número de retención en 2 o un valor más alto si tiene pensado habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino. |
| Conserve las copias de Snapshot por una cierta cantidad de días | Seleccione **mantener copias Snapshot para** y, a continuación, especifique el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas. |

Puede retener los backups de registros de archivos únicamente si seleccionó los archivos de registro de archivos como parte del backup.

8. En la página Replication, especifique la configuración de replicación:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Actualizar SnapMirror tras crear una copia Snapshot local | Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror). |
| Actualizar SnapVault después de crear una copia Snapshot local | Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Etiqueta de la política secundaria | Seleccione una etiqueta de Snapshot.<br><br>Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta.<br><br>Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria. |
| Número de reintentos con error | Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga. |

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

9. En la página Script, introduzca la ruta y los argumentos del script previo o script posterior que desea ejecutar antes o después de la operación de backup, según corresponda.

   Debe almacenar los scripts previos y los scripts posteriores en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

   También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

10. En la página Verification, realice los siguientes pasos:
    a. Seleccione la programación de backups donde desea realizar la operación de verificación.
    b. En la sección Verification script, introduzca la ruta de acceso y los argumentos del script previo o el script posterior que desea ejecutar antes o después de la operación de verificación, respectivamente.

       Debe almacenar los scripts previos y los scripts posteriores en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60

segundos.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear grupos de recursos y vincular políticas para bases de datos de Oracle

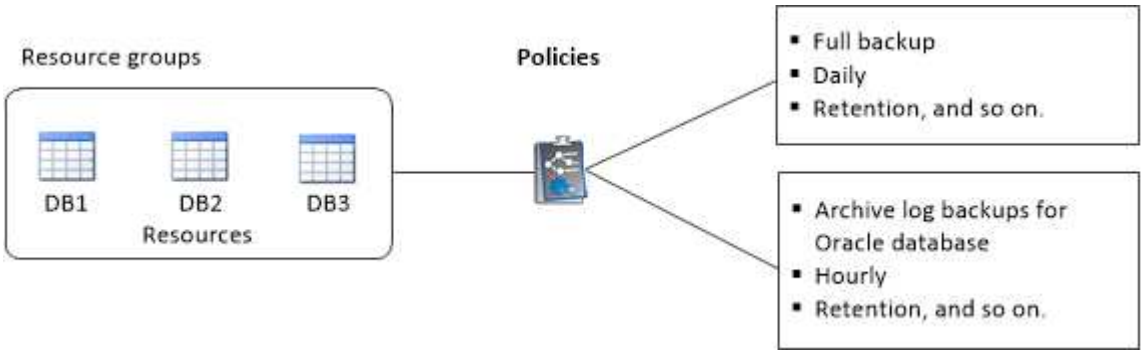
Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación.

### Acerca de esta tarea

Debe asegurarse de que la base de datos que tiene archivos en los grupos de discos ASM debe estar en estado "MOUNT" o "OPEN" para verificar sus copias de seguridad con la utilidad Oracle DBVERIFY.

Debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:




- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba un nombre para el grupo de recursos.<br>El nombre del grupo de recursos no debe superar los 250 caracteres. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Etiquetas | Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.<br><br>Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta. |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.<br><br>Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |
| Excluir destinos de registro de archivos de la copia de seguridad | Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup. |

4. En la página Resources, seleccione un nombre de host de la base de datos Oracle en la lista desplegable **Host**.

   Los recursos aparecen en la sección Available Resources solo si se detectan correctamente. Si agregó recursos recientemente, aparecerán en la lista de recursos disponibles únicamente después de actualizar la lista de recursos.

5. Seleccione los recursos de la sección Available Resources y muévalos a la sección Selected Resources.

   Puede agregar bases de datos desde hosts Linux y AIX en un solo grupo de recursos.

6. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

      También puede crear una política haciendo clic en .

      En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   b. Haga clic en En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

   c. En la ventana Add schedules for policy *policy_name*, configure la programación y haga clic en **OK**.

Donde, *policy_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

7. En la página Verification, realice los siguientes pasos:
   a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror o SnapVault y realizar la verificación en el almacenamiento secundario.
   b. Haga clic en + En la columna Configure Schedules para configurar la programación de verificación de todos los tipos de programación de la política.
   c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

| Si desea… | Realice lo siguiente… |
|---|---|
| Ejecutar la verificación después del backup | Seleccione **Ejecutar verificación después de la copia de seguridad**. |
| Programar una verificación | Seleccione **Ejecutar verificación programada** y, a continuación, seleccione el tipo de programa en la lista desplegable. |

   d. Seleccione **verificar en la ubicación secundaria** para verificar las copias de seguridad en el sistema de almacenamiento secundario.
   e. Haga clic en **Aceptar**.

   Las programaciones de verificación configuradas aparecerán en la columna Applied Schedules.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

   Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Requisitos para realizar backups de una base de datos de Oracle

Antes de realizar el backup de una base de datos de Oracle, debe asegurarse de que se hayan completado los requisitos previos.

- Debe tener creado un grupo de recursos con una política anexada.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento

secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".

- Asignó el agregado que utiliza la operación de backup a la SVM que utiliza la base de datos.
- Verificó que todos los volúmenes de datos y los volúmenes de registros de archivos que pertenecen a la base de datos están protegidos si la protección secundaria está habilitada para esa base de datos.
- Debe haber comprobado que la base de datos que contiene archivos en los grupos de discos ASM debe estar en el estado "DESMONTAR" o "ABIERTO" para verificar sus copias de seguridad con la utilidad Oracle DBVERIFY.
- Debe haber verificado que la longitud del punto de montaje del volumen no supera los 240 caracteres.
- Aumente el valor de RESTTimeout a 86400000 segundos en *C:\Program Files\NetApp \SMCore\SMCoreServiceHost.exe.config* en el host de SnapCenter Server, si la base de datos de la que se realiza el backup es grande (tamaño en TB).

  Mientras se modifican los valores, se garantiza que no haya trabajos en ejecución y se reinicia el servicio SnapCenter SMCore después de aumentar el valor.

## Realice backup de recursos de Oracle

Si un recurso no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** en la lista **View**.
3. Haga clic en y luego seleccione el nombre de host y el tipo de base de datos para filtrar los recursos.

   A continuación, puede hacer clic en para cerrar el panel de filtros.

4. Seleccione la base de datos de la que desea realizar el backup.

   Aparece la página Database-Protect.

5. En la página Resource, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.<br><br>Por ejemplo, customtext__policy_hostname o resource_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Excluir destinos de registro de archivos de la copia de seguridad | Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup. |

6. En la página Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.

      También puede crear una directiva haciendo clic en .

      En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   b. Haga clic en En la columna Configure Schedules correspondiente a la política para la cual se desea configurar una programación.
   c. En la ventana Add schedules for policy *policy_name*, configure la programación y haga clic en **OK**.

      *policy_name* es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

7. En la página Verification, realice los siguientes pasos:
   a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror o SnapVault y realizar la verificación en el almacenamiento secundario.
   b. Haga clic en En la columna Configure Schedules, a fin de configurar la programación de verificación de todos los tipos de programación de la política.
   c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Ejecutar la verificación después del backup | Seleccione **Ejecutar verificación después de la copia de seguridad**. |
| Programar una verificación | Seleccione **Ejecutar verificación programada** y, a continuación, seleccione el tipo de programa en la lista desplegable.<br>En una configuración de Flex ASM, no puede realizar la operación de verificación en los nodos Leaf si la cardinalidad es menor que el número de nodos del clúster RAC. |

   d. Seleccione **verificar en la ubicación secundaria** para verificar las copias de seguridad en el almacenamiento secundario.

e. Haga clic en **Aceptar**.

Las programaciones de verificación configuradas aparecerán en la columna Applied Schedules.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea asociar el informe de la operación de backup ejecutada en el recurso y, a continuación, seleccione **Attach Job Report**.

Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Se muestra la página de topología de la base de datos.

2. Haga clic en **copia de seguridad ahora**.
3. En la página Backup, realice los siguientes pasos:
   a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Después de terminar**

- En la configuración de AIX, puede utilizar el mandato lkdev para bloquear y el mandato rendev para cambiar el nombre de los discos en los que reside la base de datos de la que se ha realizado la copia de seguridad.

  El bloqueo o cambio de nombre de los dispositivos no afectará a la operación de restauración al restaurar mediante esa copia de seguridad.

- Si se produce un error en la operación de backup porque el tiempo de ejecución de la consulta de base de datos superó el valor de tiempo de espera, debe cambiar el valor de los parámetros ORACLE_SQL_QUERY_TIMEOUT Y ORACLE_PLUGIN_SQL_QUERY_TIMEOUT con el cmdlet Set-SmConfigSettings:

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si no se puede acceder al archivo y el punto de montaje no está disponible durante el proceso de verificación, puede que se produzca un error en la operación con el código de error DBV-00100 specified file. Debe modificar los valores de los parámetros VERIFICATION_DELAY y VERIFICATION_RETRY_COUNT en sco.properties.

Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.
- Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup.

  Para aumentar el tamaño de pila de Java, busque el archivo de script */opt/netapp/init_scripts/svservice*. En ese script, la `do_start method` Command inicia el servicio de plugin de VMware de SnapCenter. Actualice este comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

**Más información**

- "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"
- "Se omite la base de datos de Oracle RAC One Node para ejecutar operaciones de SnapCenter"
- "Se produjo un error al cambiar el estado de una base de datos de ASM de Oracle 12c"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

## Realice backups de grupos de recursos de bases de datos de Oracle

Un grupo de recursos es una agrupacion de recursos en un host o un clúster. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Resource Group** en la lista **View**.

     Puede buscar el grupo de recursos escribiendo el nombre en el cuadro de búsqueda o haciendo clic en y, a continuación, seleccionar la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.
  3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **Back up Now**.

     Si posee un grupo de recursos federado con dos bases de datos y una de ellas tiene el archivo de datos en un almacenamiento de terceros, se cancelará la operación de backup aunque la otra base de datos esté en almacenamiento de NetApp.
  4. En la página Backup, realice los siguientes pasos:
     a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

b. Haga clic en **copia de seguridad**.

5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Después de terminar**

- En la configuración de AIX, puede utilizar el mandato lkdev para bloquear y el mandato rendev para cambiar el nombre de los discos en los que reside la base de datos de la que se ha realizado la copia de seguridad.

  El bloqueo o cambio de nombre de los dispositivos no afectará a la operación de restauración al restaurar mediante esa copia de seguridad.

- Si se produce un error en la operación de backup porque el tiempo de ejecución de la consulta de base de datos superó el valor de tiempo de espera, debe cambiar el valor de los parámetros ORACLE_SQL_QUERY_TIMEOUT Y ORACLE_PLUGIN_SQL_QUERY_TIMEOUT con el cmdlet Set-SmConfigSettings:

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si no se puede acceder al archivo y el punto de montaje no está disponible durante el proceso de verificación, puede que se produzca un error en la operación con el código de error DBV-00100 specified file. Debe modificar los valores de los parámetros VERIFICATION_DELAY y VERIFICATION_RETRY_COUNT en sco.properties.

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

## Backups de bases de datos de Oracle con comandos de UNIX

El flujo de trabajo de backup incluye planificación, identificación de los recursos para el backup, creación de políticas de backup, creación de grupos de recursos y vinculación de políticas, creación de backups y supervisión de las operaciones.

**Lo que necesitará**

- Debe haber agregado las conexiones del sistema de almacenamiento y creado la credencial con los comandos *Add-SmStorageConnection* y *Add-SmCredential*.
- Estableció la sesión de conexión con el servidor SnapCenter mediante el comando *Open-SmConnection*.

  Solo puede tener una sesión iniciada con una cuenta de SnapCenter, y el token se almacena en el directorio inicial del usuario.

  La sesión de conexión solo es válida por 24 horas. Sin embargo, puede crear un token con la opción TokenNeverExpires que no caduque nunca para que la sesión sea válida siempre.

**Acerca de esta tarea**

Debe ejecutar los siguientes comandos para establecer la conexión con SnapCenter Server, detectar las instancias de la base de datos de Oracle, añadir políticas y grupos de recursos, realizar el backup y verificarlo.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".

- Pasos*
  1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado: *Open-SmConnection*
  2. Realizar la operación de detección de recursos del host: *Get-SmResources*
  3. Configure las credenciales y los nodos preferidos de la base de datos de Oracle para la operación de backup de una base de datos de RAC: *Configure-SmOracleDatabase*
  4. Cree una política de backup: *Add-SmPolicy*
  5. Recupere la información acerca de la ubicación de almacenamiento secundaria (SnapVault o SnapMirror) : *Get-SmSecondaryDetails*

     Este comando recupera los detalles de asignación de almacenamiento principal a secundario de un recurso especificado. Es posible utilizar los detalles de asignación para configurar las opciones de verificación secundaria mientras se crea un grupo de recursos de backup.
  6. Añada un grupo de recursos a SnapCenter: *Add-SmResourceGroup*
  7. Cree una copia de seguridad: *New-SmBackup*

     Puede sondear el trabajo con la opción WaitForCompletion. Si se especifica esta opción, el comando sigue sondeando el servidor hasta la finalización del trabajo de backup.
  8. Recupere los registros de SnapCenter: *Get-SmLogs*

## Supervisar las operaciones de backup de bases de datos de Oracle

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

**Acerca de esta tarea**

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Jobs**.
3. En la página Jobs, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
   d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
   e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

   Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

#### Supervise las operaciones de protección de datos en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también muestra información sobre la operación de propagación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

     Al hacer clic en una de las operaciones, se muestran sus detalles en la página Job Details.

## Cancelar las operaciones de backup de las bases de datos de Oracle

Es posible cancelar las operaciones de backup que se estén ejecutando, en cola o no respondan.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de backup.

#### Acerca de esta tarea

Cuando se cancela una operación de backup, el servidor de SnapCenter detiene la operación y quita todas las copias de Snapshot del almacenamiento si el backup creado no se registra en SnapCenter Server. Si el backup ya está registrado en el servidor SnapCenter, no retrocederá la copia de Snapshot ya creada incluso

después de que se active la cancelación.

- Solo es posible cancelar la operación de registro o backup completo que se encuentra en cola o en ejecución.
- No se puede cancelar la operación una vez iniciada la verificación.

  Si cancela la operación antes de verificarlo, se cancelará la operación y no realizará la operación de verificación.
- No se puede cancelar la operación de backup una vez que se iniciaron las operaciones de catálogo.
- Es posible cancelar una operación de backup desde la página Monitor o el panel Activity.
- Además de usar la interfaz gráfica de usuario de SnapCenter, es posible usar los comandos de la CLI para cancelar las operaciones.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
|---|---|
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione la operación y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar el trabajo de backup, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

**Resultados**

La operación se cancela y el recurso se revierte a su estado original.

Si la operación que canceló no responde en el estado de cancelación o ejecución, debe ejecutar la operación Cancel-SmJob -JobID <int> -Force para detener la operación de backup enérgicamente.

## Consulte los backups y los clones de las bases de datos de Oracle en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario.

**Acerca de esta tarea**

En la página Topology, es posible ver todos los backups y clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
- Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.
- Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

  La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

Los clones de un backup de un reflejo con versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejo no incluye el backup con versión flexible.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
  3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

     Si el recurso está protegido, se muestra la página Topology del recurso seleccionado.

  4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el almacenamiento principal y secundario.

     La sección Summary Card muestra la cantidad total de backups y clones, y la cantidad total de backups de registros.

     Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

  5. En la vista Administrar copias, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

     Estos detalles se muestran en forma de tabla.

6. Seleccione el backup en la tabla y haga clic en los iconos de protección de datos para realizar restauración, clonado, montaje, desmontaje, cambio de nombre, operaciones de catalogación, descatalogación y eliminación.

   Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

   - Si seleccionó un backup de registros, solo es posible realizar un cambio de nombre, montaje, desmontaje, catálogo, descatalogar, y eliminar operaciones.
   - Si catalogó el backup con Oracle RMAN, no puede cambiar el nombre de esos backups catalogados.

7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Si el valor asignado a SnapmirrorStatusUpdateWaitTime es menor, las copias de backup de reflejo y almacén no se enumeran en la página de topología aunque los volúmenes de registros y datos estén protegidos correctamente. Debe aumentar el valor asignado a SnapmirrorStatusUpdateWaitTime con el cmdlet *Set-SmConfigSettings* PowerShell.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*.

Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter" o. "Guía de referencia de cmdlets de SnapCenter Software".

# Montar y desmontar backups de bases de datos

Si desea acceder a los archivos en el backup, puede montar uno o varios backups de solo datos y registros. Se puede montar el backup en el mismo host donde se creó el backup o en uno remoto con el mismo tipo de configuración de host y de Oracle. Si montó manualmente los backups, debe desmontarlos manualmente después de completar la operación. En cualquier instancia determinada, se puede montar un backup de una base de datos en cualquier host. Mientras realiza una operación, puede montar un solo backup.

En una configuración de Flex ASM, no puede realizar la operación de montaje en los nodos Leaf si la cardinalidad es menor que el número de nodos del clúster RAC.

## Montar un backup de base de datos

Si desea acceder a los archivos en el backup, debe montar manualmente un backup de base de datos.

**Lo que necesitará**

- Si tiene una instancia de base de datos de Automatic Storage Management (ASM) en un entorno NFS y desea montar las copias de seguridad de ASM, debe haber agregado la ruta de acceso a los discos ASM */var/opt/snapcenter/sco/backup*/*/**/*_* en la ruta de acceso existente definida en el parámetro asm_diskstring.
- Si tiene una instancia de base de datos de ASM en un entorno NFS y desea montar los backups de registros de ASM como parte de una operación de recuperación, debe haber agregado la ruta de acceso al disco ASM */var/opt/snapcenter/scu/clones/*/** en la ruta de acceso existente definida en el parámetro

asm_diskstring.

- En el parámetro asm_diskstring, debe configurar *AFD:** si está utilizando ASMFD o configurar *ORCL:** si está utilizando ASMLIB.

> Para obtener información sobre cómo editar el parámetro asm_diskstring, consulte "Cómo agregar las rutas de acceso al disco a asm_diskstring".

- Deben configurar las credenciales de ASM y el puerto ASM si difiere del host de la base de datos de origen mientras se monta el backup.
- Si desea montar en un host alternativo, debe verificar que este host cumpla los siguientes requisitos:
  - El mismo UID y GID que el host original
  - La misma versión de Oracle que el host original
  - La misma distribución de sistema operativo que el host original
- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup compuesto por protocolos mixtos iSCSI y FC. Para obtener más información, consulte "Error en la operación porque no puede detectar el dispositivo para la LUN".
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología de la base de datos.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en el sistema de almacenamiento principal o secundario (reflejado o replicado).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Mount backups, seleccione el host en el que desea montar la copia de seguridad en la lista desplegable **Elija el host para montar la copia de seguridad**.

   Aparece la ruta de acceso de montaje */var/opt/snapcenter/sco/backup_Mount/backup_name/database_name*.

Si va a montar el backup de una base de datos de ASM, aparece la ruta de acceso de montaje +diskgroupname_SID_backupid.

1. Haga clic en **Mount**.

**Después de terminar**

- Es posible ejecutar el siguiente comando para recuperar la información relacionada con el backup montado:

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- Si montó una base de datos de ASM, puede ejecutar el siguiente comando para recuperar la información

relacionada con el backup montado:

```
./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- Para recuperar el ID de backup, ejecute el siguiente comando:

```
./sccli Get-Smbackup-BackupNamebackup_name
```

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".

### Desmontar un backup de base de datos

Es posible desmontar manualmente un backup de base de datos montado si ya no se desea acceder a los archivos en el backup.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
  3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

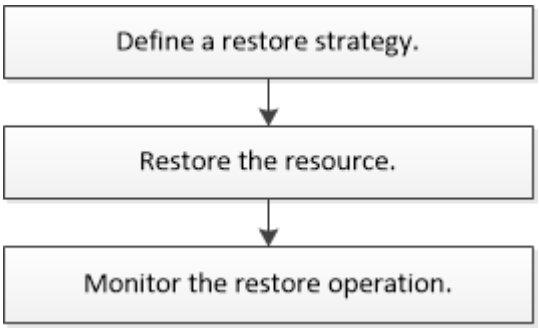
     Se muestra la página de topología de la base de datos.
  4. Seleccione el backup que está montado y haga clic en .
  5. Haga clic en **Aceptar**.

# Restaurar y recuperar bases de datos de Oracle

## Restaure el flujo de trabajo

El flujo de trabajo de restauración incluye la planificación, la realización de operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de restauración:



# Definir una estrategia de restauración y recuperación para bases de datos de Oracle

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar una base de datos.

### Tipos de backups compatibles con las operaciones de restauración y recuperación

SnapCenter admite la restauración y recuperación de diferentes tipos de backups de bases de datos de Oracle.

- Backups de datos en línea
- Backups de datos sin conexión apagados
- Backups de datos sin conexión montados
- Backup completo
- Backups sin conexión montados de bases de datos en espera de Data Guard
- Backups en línea solo de datos de bases de datos en espera de Active Data Guard

> No se pueden realizar operaciones de recuperación de bases de datos en espera de Active Data Guard.

- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración RAC
- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración ASM

### Tipos de métodos de restauración compatibles con las bases de datos de Oracle

SnapCenter es compatible con operaciones de conexión y copia y de restauración sin movimiento de bases de datos de Oracle. Durante una operación de restauración, SnapCenter determina el método de restauración adecuado del sistema de archivos que se usará para restaurar sin pérdida de datos.

> SnapCenter no es compatible con SnapRestore basado en volúmenes.

#### Restauración por conexión y copia

Si el diseño de la base de datos difiere del backup o si se agregan archivos nuevos después de la creación del backup, se ejecuta una restauración por conexión y copia. En el método de restauración por conexión y copia, se ejecutan las siguientes tareas:

- Pasos*
  1. Se clona el volumen a partir de la copia de Snapshot, y se construye la pila del sistema de archivos en el host con los LUN o volúmenes clonados.
  2. Se copian los archivos de los sistemas de archivos clonados en los sistemas de archivos originales.
  3. Los sistemas de archivos clonados luego se desmontan del host, y se eliminan los volúmenes clonados de ONTAP.

Para una configuración de Flex ASM (donde la cardinalidad es inferior al número de nodos del clúster de RAC) o bases de datos de RAC de ASM en VMDK o RDM, solo se admite el método de restauración por conexión y copia.

Aunque se haya habilitado una restauración sin movimiento forzada, SnapCenter ejecuta la restauración por conexión y copia en las siguientes situaciones:

- Restauración desde el sistema de almacenamiento secundario, si Data ONTAP corresponde a una versión anterior a 8.3
- Restauración de grupos de discos de ASM en nodos de una configuración de Oracle RAC en la cual no está configurada la instancia de base de datos
- En una configuración de Oracle RAC, en cualquiera de los nodos del mismo nivel si la instancia de ASM o del clúster no están en ejecución o si el nodo del mismo nivel está inactivo
- Restauración de los archivos de control únicamente
- Restauración de un subconjunto de espacios de tablas que residen en un grupo de discos de ASM
- Grupo de discos compartido entre archivos de datos, archivo sp y archivo de contraseñas
- Servicio de SnapCenter Plug-in Loader (SPL) no instalado o sin ejecución en el nodo remoto de un entorno RAC
- Adición de nuevos nodos a Oracle RAC sin que SnapCenter Server reciba información sobre los nuevos nodos agregados

#### Restauración sin movimiento

Si el diseño de la base de datos es similar al backup y no hubo ningún cambio de configuración en el almacenamiento ni en la pila de base de datos, se ejecuta una restauración sin movimiento, en la cual se restauran el archivo o el LUN en ONTAP. SnapCenter es compatible únicamente con SnapRestore de archivo único (SFSR) como parte del método de restauración sin movimiento.

Data ONTAP 8.3 o y versiones posteriores son compatibles con la restauración sin movimiento desde una ubicación secundaria.

Si se desea ejecutar una restauración sin movimiento en la base de datos, es necesario confirmar que solo haya archivos de datos en el grupo de discos de ASM. Se debe crear un backup cada vez que se hacen cambios en el grupo de discos de ASM o en la estructura física de la base de datos. Después de ejecutar una restauración sin movimiento, el grupo de discos contendrá la misma cantidad de archivos de datos que había en el momento del backup.

La restauración sin movimiento se aplica automáticamente cuando el grupo de discos o el punto de montaje cumple los siguientes criterios:

- No se agregan nuevos archivos de datos después del backup (control de archivos externo).
- No se agregan, eliminan ni recrean discos de ASM o LUN después del backup (control de cambios estructurales del grupo de discos de ASM).
- No se agregan, eliminan ni recrean LUN en el grupo de discos de LVM (control de cambios estructurales del grupo de discos de LVM).

También es posible habilitar una restauración sin movimiento forzada desde la interfaz gráfica de usuario, desde la interfaz de línea de comandos de SnapCenter o desde el cmdlet de PowerShell para anular el control de archivos externo y el control de cambios estructurales del grupo de discos de LVM.

### Restauración sin movimiento en RAC de ASM

En SnapCenter, el nodo en el que se ejecuta la restauración se denomina nodo primario, y los demás nodos de RAC donde reside el grupo de discos de ASM se denominan nodos del mismo nivel. SnapCenter cambia el estado del grupo de discos de ASM a desmontaje en todos los nodos donde el grupo de discos de ASM tiene estado de montaje antes de ejecutar la operación de restauración de almacenamiento. Una vez que se termina de restaurar el almacenamiento, SnapCenter cambia el estado del grupo de discos de ASM al que tenía antes de la operación de restauración.

En los entornos DE SAN, SnapCenter quita los dispositivos de todos los nodos del mismo nivel y ejecuta la operación de anulación de asignación de LUN antes de la operación de restauración de almacenamiento. Después de la operación de restauración de almacenamiento, SnapCenter ejecuta una operación de asignación de LUN y construye los dispositivos en todos los nodos del mismo nivel. En un entorno DE SAN, si el diseño de ASM de Oracle RAC reside en LUN, durante la restauración SnapCenter ejecuta operaciones para desasignar LUN, restaurar LUN y asignar LUN en todos los nodos del clúster de RAC donde reside el grupo de discos de ASM. En la restauración, incluso si no todos los iniciadores de los nodos de RAC se usaban para los LUN, después de restaurar, SnapCenter crea un iGroup nuevo con todos los iniciadores de todos los nodos de RAC.

- Si hay algún fallo durante la actividad previa a la restauración en los nodos del mismo nivel, SnapCenter revierte automáticamente el estado del grupo de discos de ASM al usado antes de restaurar en los nodos del mismo nivel donde la operación previa a la restauración se ejecutó correctamente. No es posible revertir el nodo primario y el nodo del mismo nivel en los que falló la operación. Antes de intentar otra restauración, se debe reparar manualmente el problema en el nodo del mismo nivel y colocar el grupo de discos de ASM del nodo primario nuevamente en el estado de montaje.
- Si hay algún fallo durante la actividad de restauración, la operación de restauración falla y no se ejecuta la reversión. Antes de intentar otra restauración, se debe reparar manualmente el problema de restauración del almacenamiento y colocar el grupo de discos de ASM del nodo primario nuevamente en el estado de montaje.
- Si hay algún fallo durante la actividad posterior a la restauración en cualquiera de los nodos del mismo nivel, SnapCenter avanza con la operación de restauración en los demás nodos del mismo nivel. Es necesario reparar manualmente el problema posterior a la restauración en el nodo del mismo nivel.

### Tipos de operaciones de restauración compatibles con las bases de datos de Oracle

SnapCenter permite ejecutar diferentes tipos de operaciones de restauración para las bases de datos de Oracle.

Antes de restaurar la base de datos, se validan los backups para identificar si faltan archivos al compararlos con los archivos de la base de datos real.

#### Restauración completa

- Solo restaura los archivos de datos
- Solo restaura los archivos de control
- Restaura los archivos de datos y los archivos de control

- Restaura archivos de datos, archivos de control y archivos de registro de recuperación en las bases de datos en espera de Data Guard y Active Data Guard

#### Restauración parcial

- Restaura solo los espacios de tablas seleccionados
- Restaura solo las bases de datos conectables (PDB) seleccionadas
- Restaura solo los espacios de tablas seleccionados de una PDB

### Tipos de operaciones de recuperación compatibles con las bases de datos de Oracle

SnapCenter permite ejecutar diferentes tipos de operaciones de recuperación para las bases de datos de Oracle.

- La base de datos hasta la última transacción (todos los registros)
- La base de datos hasta un número de cambio de sistema específico (SCN)
- La base de datos hasta una fecha y hora específicas

  La fecha y la hora de la recuperación deben especificarse según la zona horaria del host de la base de datos.

  SnapCenter también incluye la opción no recovery para las bases de datos de Oracle.

> El plugin para la base de datos de Oracle no es compatible con la recuperación si se hizo una restauración con un backup creado con el rol de base de datos en espera. Para las bases de datos físicas en espera, siempre se debe usar la recuperación manual.

### Limitaciones de la restauración y la recuperación de bases de datos de Oracle

Antes de ejecutar operaciones de restauración y recuperación, es necesario conocer las limitaciones.

Si está utilizando cualquier versión de Oracle de 11.2.0.4 a 12.1.0.1, la operación de restauración estará en estado de bloqueo cuando ejecute el comando *renamedg* . Puede aplicar el parche de Oracle 19544733 para solucionar este problema.

No se admiten las siguientes operaciones de restauración y recuperación:

- Restauración y recuperación de espacios de tablas en la base de datos del CDB raíz
- Restauración de espacios de tablas temporales y asociados con PDB
- Restauración y recuperación de espacios de tablas de varios PDB simultáneamente
- Restauración de backups de registros
- Restauración de backups en otra ubicación
- Restauración de archivos de registro de recuperación en cualquier configuración, excepto bases de datos en espera de Data Guard o de Active Data Guard
- Restauración de archivos SPFILE y Password
- Cuando se ejecuta una operación de restauración en una base de datos que se volvió a crear con el nombre de base de datos preexistente en el mismo host, fue gestionado por SnapCenter y tenía backups válidos, la operación de restauración sobrescribe los archivos de base de datos recién creados aunque los DBID sean diferentes.

Esto se puede evitar realizando una de las siguientes acciones:

- Detectar los recursos de SnapCenter después de volver a crear la base de datos
- Cree una copia de seguridad de la base de datos que se ha vuelto a crear

**Limitaciones relacionadas con la recuperación de espacios de tablas en un momento específico**

- No se admite la recuperación puntual (PITR) de los tablespaces SYSTEM, SYSAUX y UNDO
- No se pueden realizar PITR de tablespaces junto con otros tipos de restauraciones
- Si se cambia el nombre de un tablespace y se desea recuperarlo a un punto antes de cambiar su nombre, debe especificar el nombre anterior del tablespace
- Si las restricciones de las tablas de un tablespace se encuentran en otro tablespace, debe recuperar los dos tablespaces
- Si una tabla y sus índices se almacenan en tablespaces diferentes, los índices se deben eliminar antes de ejecutar PITR
- PITR no se puede utilizar para recuperar el tablespace por defecto actual
- PITR no se puede utilizar para recuperar tablespaces que contengan cualquiera de los siguientes objetos:
  - Objetos con objetos subyacentes (como vistas materializadas) o objetos contenidos (como tablas particionadas) a menos que todos los objetos subyacentes o contenidos estén en el conjunto de recuperación

    Además, si las particiones de una tabla con particiones se almacenan en distintos tablespaces, debe eliminar la tabla antes de realizar PITR o mover todas las particiones al mismo tablespace antes de realizar PITR.

  - Deshacer o revertir segmentos
  - Colas avanzadas compatibles con Oracle 8 con varios destinatarios
  - Objetos propiedad del usuario SYS

    Ejemplos de estos tipos de objetos son PL/SQL, clases Java, programas de llamada, vistas, sinónimos, usuarios, privilegios, dimensiones, directorios y secuencias.

## Orígenes y destinos para restaurar bases de datos de Oracle

Es posible restaurar una base de datos de Oracle desde una copia de backup en el almacenamiento primario o el almacenamiento secundario. Las bases de datos se pueden restaurar únicamente en la misma ubicación y en la misma instancia de base de datos. Sin embargo, en la configuración de RAC, se pueden restaurar bases de datos a otros nodos.

#### Orígenes para operaciones de restauración

Es posible restaurar bases de datos desde un backup en el almacenamiento primario o el almacenamiento secundario. Si desea restaurar desde un backup en el almacenamiento secundario en una configuración de reflejos múltiples, puede seleccionar el reflejo de almacenamiento secundario como origen.

#### Destinos para operaciones de restauración

Las bases de datos se pueden restaurar únicamente en la misma ubicación y en la misma instancia de base de datos.

En una configuración de RAC, se pueden restaurar bases de datos de RAC desde cualquier nodo en el clúster.

## Requisitos para restaurar una base de datos de Oracle

Antes de restaurar una base de datos de Oracle, debe asegurarse de que se hayan completado los requisitos previos.

- Definió la estrategia de restauración y recuperación.
- El administrador de SnapCenter asignó SVM para los volúmenes de origen y los volúmenes de destino si va a replicar copias de Snapshot a un reflejo o un almacén.
- Si se reducen los archivos de registro como parte del backup, debe haber montado manualmente los backups de los archivos de registro requeridos.
- Si desea restaurar bases de datos de Oracle que residen en un VMDK, debe asegurarse de que la máquina invitada tenga la cantidad requerida de ranuras libres para asignar los VMDK clonados.
- Se aseguró de que todos los volúmenes de datos y los volúmenes de registros de archivos que pertenecen a la base de datos estén protegidos si la protección secundaria está habilitada para esa base de datos.
- Debe asegurarse de que la base de datos RAC One Node se encuentra en estado "nomount" para realizar una restauración completa de archivos de control o de bases de datos.
- Si tiene una instancia de base de datos de ASM en el entorno NFS, debe añadir la ruta de acceso al disco de ASM */var/opt/snapcenter/scu/clones/*/** a la ruta de acceso existente definida en el parámetro asm_diskstring de modo que pueda montar correctamente los backups de registro de ASM como parte de la operación de recuperación.
- En el parámetro asm_diskstring, debe configurar *AFD:** si está utilizando ASMFD o configurar *ORCL:** si está utilizando ASMLIB.

  Para obtener información sobre cómo editar el parámetro asm_diskstring, consulte "Cómo agregar las rutas de acceso al disco a asm_diskstring"

- Debe configurar el listener estático en el archivo **listener.ora** disponible en *$ORACLE_HOME/network/admin* para bases de datos que no son de ASM y *$GRID_HOME/network/admin* para bases de datos de ASM si ha deshabilitado la autenticación del sistema operativo y ha habilitado la autenticación de base de datos de Oracle para una base de datos de Oracle, y desea restaurar los archivos de datos y archivos de control de esa base de datos.
- Debe aumentar el valor del parámetro SCORestoreTimeout. Para hacerlo, ejecute el comando Set-SmConfigSettings si el tamaño de la base de datos está en terabytes (TB).
- Asegúrese de que todas las licencias requeridas para vCenter estén instaladas y actualizadas.

  Si las licencias no están instaladas o actualizadas, aparecerá un mensaje de advertencia. Si ignora la advertencia y continúa, se produce un error en la restauración desde RDM.

- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup compuesto por protocolos mixtos iSCSI y FC. Para obtener más información, consulte "Error en la operación porque no puede detectar el dispositivo para la LUN".

## Restaurar base de datos de Oracle

En caso de pérdida de datos, es posible usar SnapCenter para restaurar datos desde

uno o más backups en el sistema de archivos activo para luego recuperar la base de datos.

**Acerca de esta tarea**

La recuperación se lleva a cabo con los registros de archivos disponibles en la ubicación del registro de archivos configurado. Si los registros de archivos requeridos para la recuperación no están disponibles en la ubicación configurada, debe montar la copia Snapshot que contiene los registros y especificar la ruta como registros de archivo externos.

Si se migra la base de datos de ASM de ASMLIB a ASMFD, los backups creados con ASMLIB no se pueden utilizar para restaurar la base de datos. Es necesario crear backups en la configuración de ASMFD y utilizar esos backups para restaurar. De forma similar, si se migra la base de datos de ASM de ASMFD a ASMLIB, es necesario crear backups en la configuración de ASMLIB para restaurar.

Cuando restaura una base de datos, se crea un archivo de bloqueo operativo (.sm_lock_dbsid) en el host de la base de datos de Oracle, en el directorio $ORACLE_HOME/DBS, para evitar que se ejecuten varias operaciones en la base de datos. Después de restaurar la base de datos, se elimina automáticamente el archivo de bloqueo operativo.

No se admite la restauración de archivos SPFILE y Password.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología de la base de datos.

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:

   a. Si seleccionó un backup de una base de datos en un entorno RAC, seleccione el nodo de RAC.

   b. Al seleccionar un datos reflejados o de almacén:

      - si no hay backup de registros en el reflejo o el almacén, no se selecciona nada y los localizadores están vacíos.
      - si existen backups de registros en el reflejo o almacén, se selecciona el último backup de registros y se muestra el localizador correspondiente.

        Si el backup de registro seleccionado existe en la ubicación de reflejo y almacén, se muestran ambos localizadores.

   c. Realice las siguientes acciones:

| Si desea restaurar… | Realice lo siguiente… |
| --- | --- |
| Todos los archivos de datos de la base de datos | Seleccione **todos los archivos de datos**.<br><br>Solo se restauran los archivos de datos de la base de datos. No se restauran los archivos de control, los registros de archivos ni los archivos de registro de recuperación. |
| Espacios de tabla | Seleccione **Tablespaces**.<br><br>Se pueden especificar los espacios de tabla que se desean restaurar. |
| Archivos de control | Seleccione **Archivos de control**.<br><br>Al restaurar los archivos de control, asegúrese de que la estructura de directorio existe o se debe crear con las propiedades de usuario y grupo correctas, si las hay, para permitir que los archivos se copien a la ubicación de destino mediante el proceso de restauración. Si no existe el directorio, se producirá un error en el trabajo de restauración. |
| Archivos de registro de recuperación | Seleccione **Redo log files**.<br><br>Esta opción está disponible solo para bases de datos Data Guard en espera o Active Data Guard en espera.<br><br>No se realiza un backup de los archivos de registro de recuperación para bases de datos que no son de Data Guard. Para bases de datos que no son de Data Guard, la recuperación se realiza con registros de archivos. |
| Bases de datos conectables (PDB) | Seleccione **Pluggable databases** y, a continuación, especifique las PDB que desea restaurar. |

| Si desea restaurar… | Realice lo siguiente… |
| --- | --- |
| Espacios de tabla de bases de datos conectables (PDB) | Seleccione * tablespaces de base de datos conectables (PDB)* y, a continuación, especifique la PDB y los tablespaces de esa PDB que desea restaurar.<br><br>Esta opción está disponible solo si seleccionó una PDB para restaurar. |

d. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.

   Los distintos estados de una base de datos, del más alto al más bajo, son open, mounted, started y shutdown. Debe seleccionar esta casilla de comprobación si la base de datos está en un estado más alto, pero el estado debe cambiarse a un estado más bajo para realizar una operación de restauración. Si la base de datos está en un estado más bajo, pero el estado debe cambiarse a uno más alto para realizar la operación de restauración, el estado de la base de datos se modifica automáticamente aunque no seleccione la casilla de comprobación.

Si una base de datos está en el estado open y, para restaurarla, la base de datos necesita que esté en el estado mounted, el estado de la base de datos se modifica únicamente si selecciona esta casilla de comprobación.

a. Seleccione **Force in place restore** si desea realizar restauraciones in situ en los escenarios en los que se agregan nuevos archivos de datos después de la copia de seguridad o cuando se agregan, eliminan o recrean LUN en un grupo de discos de LVM.

7. En la página Recovery Scope, realice las siguientes acciones:

| Si… | Realice lo siguiente… |
| --- | --- |
| Desea recuperar la última transacción | Seleccione **todos los registros**. |
| Desea recuperar a un número de cambio de sistema (SCN) específico | Seleccione **Until SCN (System Change Number)**. |
| Desea recuperar a una fecha y una hora específicas | Seleccione **Fecha y hora**.<br><br>Debe especificar la fecha y la hora de la zona horaria del host de la base de datos. |
| No desea recuperar | Seleccione **sin recuperación**. |

| Si… | Realice lo siguiente… |
| --- | --- |
| Desea especificar cualquier ubicación de registros de archivos externos | Seleccione **especifique las ubicaciones de los archivos de registro externos** y, a continuación, especifique la ubicación de los archivos de registro de archivos externos.<br><br>Si se reducen los registros de archivos como parte del backup y se montaron manualmente los backups de los registros de archivo requeridos, debe especificar la ruta de acceso del backup montado como ubicación de registro de archivo externo para la recuperación.<br><br>• "Protección de datos de Oracle con ONTAP"<br>• "Se produce un error en el funcionamiento con ORA-00308" |

No se pueden realizar restauraciones con recuperación de backups secundarios si los volúmenes de registros de archivos no están protegidos y los volúmenes de datos sí lo están. Sólo puede restaurar seleccionando **sin recuperación**.

Si se va a recuperar una base de datos de RAC con la opción de base de datos abierta seleccionada, solo la instancia de RAC en la que se inició la operación de recuperación vuelve a estar en estado abierto.

No se admite la recuperación para bases de datos Data Guard en espera y Active Data Guard en espera.

8. En la página PreOps, introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de restauración.

   Debe almacenar los scripts previos en la ruta de acceso */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de ella. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

   También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

9. En la página PostOps, siga estos pasos:

   a. Introduzca la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de restauración.

      Debe almacenar los scripts posteriores en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

   b. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.

      Después de restaurar una base de datos de contenedor (CDB) con o sin archivos de control, o

después de restaurar solo los archivos de control de la CDB, si especifica que se abre la base de datos después de la recuperación, solo se abre la CDB y no las bases de datos conectables (PDB) de esa CDB.

En una configuración de RAC, solo la instancia de RAC que se usa para la recuperación se abre después de esta.

> Después de restaurar un espacio de tabla de usuario con archivos de control, un espacio de tabla del sistema con o sin archivos de control o una PDB con o sin archivos de control, solo el estado de la PDB relacionada con la operación de restauración vuelve a su estado original. El estado de las demás PDB que no se usaron para la restauración no vuelven a su estado original, ya que el estado de esas PDB no se guardó. Debe modificar manualmente el estado de las PDB que no se usaron para la restauración.

10. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.

    También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de restauración realizada, debe seleccionar **Adjuntar informe de trabajo**.

> Para la notificación por correo electrónico, debe haber especificado los detalles del servidor SMTP a través de la interfaz gráfica de usuario o el comando Set-SmSmtpServer de PowerShell.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.
2. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Para más información**

- "Se omite la base de datos de Oracle RAC One Node para ejecutar operaciones de SnapCenter"
- "Error al restaurar desde una ubicación de SnapMirror o SnapVault secundaria"
- "Se ha producido un error al restaurar desde un backup de una encarnación huérfana"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

## Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico

Se puede restaurar un subconjunto de espacios de tablas que se han dañado o eliminado sin afectar a los otros espacios de tablas de la base de datos. SnapCenter utiliza RMAN para realizar una recuperación puntual (PITR) de los tablespaces.

**Lo que necesitará**

Los backups necesarios para ejecutar PITR de espacios de tablas deben catalogarse y montarse.

**Acerca de esta tarea**

Durante la operación PITR, RMAN crea una instancia auxiliar en el destino auxiliar especificado. El destino auxiliar puede ser un punto de montaje o un grupo de discos ASM. Si hay suficiente espacio en la ubicación

montada, puede reutilizar una de las ubicaciones montadas en lugar de un punto de montaje dedicado.

Debe especificar la fecha y hora o SCN y el espacio de tabla se restaurará en la base de datos de origen.

Se pueden seleccionar y restaurar varios espacios de tablas que residen en entornos ASM, NFS y SAN. Por ejemplo, si los espacios de tablas TS2 y TS3 residen en NFS y TS4 en SAN, puede realizar una única operación PITR para restaurar todos los espacios de tablas.

En una configuración de RAC, puede realizar PITR de tablespaces desde cualquier nodo del RAC.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos del tipo de instancia única (Multitenant) ya sea en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología de la base de datos.

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).

   Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione el backup catalogado y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
   a. Si seleccionó un backup de una base de datos en un entorno RAC, seleccione el nodo de RAC.
   b. Seleccione **Tablespaces** y, a continuación, especifique los tablespaces que desea restaurar.

      No puede realizar PITR en tablespaces SYSAUX, SYSTEM y UNDO.

   c. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.
7. En la página Recovery Scope, realice una de las siguientes acciones:
   - Si desea recuperar un número de cambio de sistema (SCN) específico, seleccione **hasta SCN** y especifique el SCN y el destino auxiliar.
   - Si desea recuperar una fecha y hora específicas, seleccione **Fecha y hora** y especifique la fecha y hora y el destino auxiliar. Cuando especifica el SCN o la fecha y hora, SnapCenter enumera los backups necesarios para ejecutar PITR, pero no se catalogan y montan.
8. En la página PreOps, introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de restauración.

   Debe almacenar los scripts previos en la ruta de acceso /var/opt/snapcenter/spl/scripts o en cualquier carpeta dentro de ella. De forma predeterminada, se completa la ruta de acceso /var/opt/snapcenter/spl/scripts. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar

los scripts, debe especificar esas carpetas en la ruta.

También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

1. En la página PostOps, siga estos pasos:
   a. Introduzca la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de restauración.
   b. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.
2. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.
3. Revise el resumen y, a continuación, haga clic en **Finalizar**.
4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Restaure y recupere una base de datos conectable mediante la recuperación de un momento específico

Puede restaurar y recuperar una base de datos conectables (PDB) que se dañó o se borró sin afectar a las otras PDB de la base de datos de contenedores (CDB). SnapCenter utiliza RMAN para realizar una recuperación de un momento específico (PITR) de la PDB.

**Lo que necesitará**

Los backups necesarios para ejecutar PITR de una PDB deben catalogarse y montarse.

> En una configuración de RAC, debe cerrar manualmente la PDB (cambiando el estado a MONTADO) en todos los nodos de la configuración de RAC.

**Acerca de esta tarea**

Durante la operación PITR, RMAN crea una instancia auxiliar en el destino auxiliar especificado. El destino auxiliar puede ser un punto de montaje o un grupo de discos ASM. Si hay suficiente espacio en la ubicación montada, puede reutilizar una de las ubicaciones montadas en lugar de un punto de montaje dedicado.

Debe especificar la fecha y hora o SCN para ejecutar PITR de la PDB. RMAN puede recuperar PDB de LECTURA, SOLO LECTURA o PDB borrada, incluidos archivos de datos.

Solo puede restaurar y recuperar:

- Una PDB a la vez
- Un tablespace en una PDB
- Varios espacios de tablas de la misma PDB

> En una configuración de RAC, puede realizar PITR de tablespaces desde cualquier nodo del RAC.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos del tipo de instancia única (Multitenant) ya sea en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología de la base de datos.

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).

   Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione el backup catalogado y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
   a. Si seleccionó un backup de una base de datos en un entorno RAC, seleccione el nodo de RAC.
   b. Según si desea restaurar la PDB o los espacios de tablas en una PDB, realice una de las acciones:

| Si desea… | Pasos… |
|---|---|
| Restaurar una PDB | i. Seleccione **bases de datos conectables (PDB)**.<br>ii. Especifique la PDB que desea restaurar.<br>No se puede ejecutar PITR en la base de datos PDB$SEED. |
| Restaurar espacios de tablas en una PDB | i. Seleccione **tablespaces de base de datos conectables (PDB)**.<br>ii. Especifique la PDB.<br>iii. Especifique un único espacio de tabla o varios espacios de tablas que desee restaurar.<br>No puede realizar PITR en tablespaces SYSAUX, SYSTEM y UNDO. |

   c. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.
7. En la página Recovery Scope, realice una de las siguientes acciones:
   - Si desea recuperar un número de cambio de sistema (SCN) específico, seleccione **hasta SCN** y

especifique el SCN y el destino auxiliar.

- Si desea recuperar una fecha y hora específicas, seleccione **Fecha y hora** y especifique la fecha y hora y el destino auxiliar. Cuando especifica el SCN o la fecha y hora, SnapCenter enumera los backups necesarios para ejecutar PITR, pero no se catalogan y montan.

8. En la página PreOps, introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de restauración.

   Debe almacenar los scripts previos en la ruta de acceso /var/opt/snapcenter/spl/scripts o en cualquier carpeta dentro de ella. De forma predeterminada, se completa la ruta de acceso /var/opt/snapcenter/spl/scripts. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

1. En la página PostOps, siga estos pasos:
   a. Introduzca la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de restauración.
   b. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.

      En una configuración de RAC, la PDB solo se abre en el nodo donde se recuperó la base de datos. Debe abrir manualmente la PDB recuperada en todos los demás nodos de la configuración de RAC.

2. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.
3. Revise el resumen y, a continuación, haga clic en **Finalizar**.
4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Restaure y recupere bases de datos de Oracle con comandos de UNIX

El flujo de trabajo de restauración y recuperación incluye la planificación, la realización de operaciones de restauración y recuperación, y la supervisión de las operaciones.

**Acerca de esta tarea**

Debe ejecutar los siguientes comandos para establecer la conexión con SnapCenter Server, enumerar los backups y recuperar su información, y restaurar el backup.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".

- Pasos*

1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado: *Open-SmConnection*
2. Recupere la información sobre los backups que desea restaurar: *Get-SmBackup*
3. Recupere la información detallada acerca del backup especificado: *Get-SmBackupDetails*

   Este comando recupera la información detallada sobre el backup de un recurso especificado con un

determinado ID de backup. La información incluye nombre de la base de datos, versión, inicio, SCN de inicio y de finalización, espacios de tabla, bases de datos conectables y sus espacios de tabla.

4. Restaure los datos del backup: *Restore-SmBackup*

## Supervisar las operaciones de restauración de bases de datos de Oracle

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

**Acerca de esta tarea**

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

## Cancelar operaciones de restauración de bases de datos de Oracle

Es posible cancelar los trabajos de restauración que se encuentran en cola.

Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.

**Acerca de esta tarea**

- Es posible cancelar una operación de restauración en cola desde la página Monitor o el panel Activity.
- No se puede cancelar una operación de restauración en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está desactivado para operaciones de restauración que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de restauración en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione el trabajo y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar la operación de restauración, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

# Clone la base de datos de Oracle

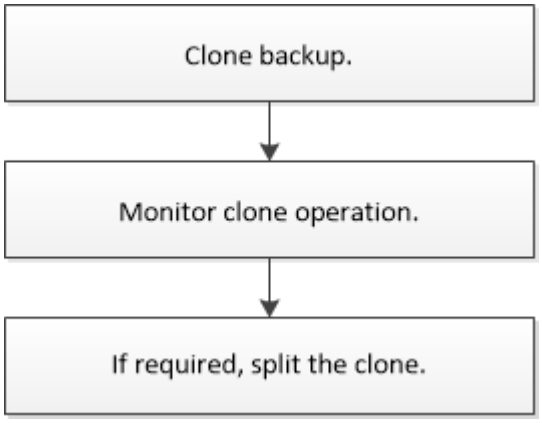
## Flujo de trabajo de clonado

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

Pueden clonarse bases de datos por los siguientes motivos:

- Para poner a prueba una funcionalidad que debe implementarse con la estructura y el contenido de la base de datos actual durante ciclos de desarrollo de aplicaciones.
- Para completar almacenes de datos con herramientas de extracción y manipulación de datos.
- Para recuperar datos que se eliminaron o se modificaron por error.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de clonado:




## Defina una estrategia de clonado para bases de datos de Oracle

Definir una estrategia antes de clonar una base de datos permite garantizar que la operación se ejecute correctamente.

### Tipos de backups compatibles con la clonado

SnapCenter permite clonar diversos tipos de backup de las bases de datos de Oracle.

- Backups de datos en línea
- Backup completo en línea
- Backups de montaje sin conexión
- Backups de apagado sin conexión
- Backups de bases de datos en espera de Data Guard y bases de datos en espera de Active Data Guard
- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración RAC
- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración ASM

No se admite la configuración de Oracle ASM si la opción USER_Friendly_Names del archivo de configuración multivía está establecida en yes y los alias o enlaces simbólicos se definen para los discos ASM de Oracle que utilizan el archivo de reglas udev.

No se admite la clonado de backups de registros de archivos.

**Tipos de clonado compatibles con las bases de datos de Oracle**

En un entorno de bases de datos de Oracle, SnapCenter admite la clonado de un backup de base de datos. Puede clonar el backup de sistemas de almacenamiento primarios y secundarios.

El servidor SnapCenter utiliza la tecnología FlexClone de NetApp para clonar backups.

Puede actualizar un clon ejecutando el comando "Refresh-SmClone". Este comando crea un backup de la base de datos, elimina el clon existente y crea un clon con el mismo nombre.

La operación de actualización de clones solo puede realizarse con los comandos UNIX.

**Convenciones de nomenclatura de los clones para las bases de datos de Oracle**

A partir de SnapCenter 3.0, la convención de nomenclatura utilizada para los clones de sistemas de archivos es diferente de la aplicada a los clones de grupos de discos de ASM.

- La convención de nomenclatura para los sistemas de archivos SAN o NFS es FileSystemNameofsourcedatabase_CLONESID.
- La convención de nomenclatura para los grupos de discos de ASM es SC_HASHCODEofDISKGROUP_CLONESID.

  HASHCODEofDISKGROUP es un número generado automáticamente (de 2 a 10 dígitos) exclusivo para cada grupo de discos de ASM.

**Limitaciones de la clonado de bases de datos de Oracle**

Antes de clonar las bases de datos, es necesario tener en cuenta las limitaciones de las operaciones de clonado.

- Si utiliza una versión de Oracle de 11.2.0.4 a 12.1.0.1, la operación de clonado estará en estado colgado al ejecutar el comando *renamedg* . Puede aplicar el parche de Oracle 19544733 para solucionar este problema.
- No se admite la clonado de bases de datos de un LUN conectado directamente a un host (por ejemplo, usando el iniciador de iSCSI de Microsoft en un host de Windows) a un VMDK o un LUN de RDM en el mismo host de Windows, ni en otro host de Windows, o viceversa.
- El directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- Si se mueve un LUN que contiene un clon de un volumen nuevo, no es posible eliminar el clon.

## Requisitos para clonar una base de datos de Oracle

Antes de clonar una base de datos de Oracle, debe asegurarse de que se hayan completado los requisitos previos.

- Creó un backup de la base de datos con SnapCenter.

  Debe haber creado correctamente backups del registro y de datos en línea, o backups sin conexión (montados o apagados) para que la operación de clonado se complete correctamente.

- Si desea personalizar las rutas de acceso del archivo de control o el archivo de registro de recuperación, debe haber aprovisionado previamente el sistema de archivos requerido o el grupo de discos de Automatic Storage Management (ASM).

  De forma predeterminada, los archivos de registro de recuperación y de control de la base de datos clonada se crean en el grupo de discos de ASM o el sistema de archivos aprovisionado por SnapCenter para los archivos de datos de la base de datos del clon.

- Si está usando ASM sobre NFS, debe agregar */var/opt/snapcenter/scu/clones///** a la ruta de acceso existente definida en el parámetro asm_diskstring.
- En el parámetro asm_diskstring, debe configurar *AFD:** si está utilizando ASMFD o configurar *ORCL:** si está utilizando ASMLIB.

  Para obtener información sobre cómo editar el parámetro asm_diskstring, consulte "Cómo agregar las rutas de acceso al disco a asm_diskstring".

- Si crea el clon en un host alternativo, este host debe cumplir los siguientes requisitos:
  - El plugin de SnapCenter para base de datos de Oracle debe estar instalado en el host alternativo.
  - El host del clon debe poder detectar LUN de almacenamiento principal o secundario.
    - Si clona un almacenamiento principal o secundario (almacén o reflejo) en un host alternativo, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento secundario y el host alternativo, o una zona adecuada para Fibre Channel (FC).
    - Si clona un almacén o un reflejo en el mismo host, asegúrese de que se establezca una sesión iSCSI entre el almacén o reflejo y el host, o una zona adecuada para FC.
    - Si clona en un entorno virtualizado, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento principal o secundario y el servidor ESX que aloja al host alternativo, o una zona adecuada para FC.

      Para obtener más información, consulte "documentación de utilidades de host".
  - Si la base de datos de origen es una base de datos ASM:
    - La instancia de ASM debe estar activa y en ejecución en el host donde se realizará el clon.
    - El grupo de discos ASM debe aprovisionarse antes de la operación de clonado si desea colocar archivos de registro de archivos de la base de datos clonada en un grupo de discos de ASM dedicado.
    - Que el nombre del grupo de discos de datos pueda configurarse y, a la vez, que ningún otro grupo de discos ASM use el nombre en el host donde se realizará la clonado.

      Los archivos de datos que residen en el grupo de discos ASM se aprovisionan como parte del flujo de trabajo del clon de SnapCenter.

- El tipo de protección del LUN de datos y el LUN de registro, como reflejo, almacén o reflejo-almacén, debe ser el mismo para detectar localizadores secundarios durante la clonado en un host alternativo que use backups de registros.
- Configuró el valor de exclude_seed_cdb_view como FALSE en el archivo de parámetros de la base de datos de origen con el fin de recuperar información relacionada con la PDB de inicialización para la

clonado de una base de datos de 12*c*.

La PDB de inicialización es una plantilla proporcionada por el sistema que la CDB puede utilizar para crear PDB. La PDB de inicialización se denomina PDB$SEED. Para obtener información sobre PDB$SEED, consulte el ID de documento de Oracle 1940806.1.

Debe configurar el valor antes de realizar una copia de seguridad de la base de datos 12*c*.

- SnapCenter admite copia de seguridad de sistemas de archivos administrados por el subsistema autofs. Si va a clonar la base de datos, asegúrese de que los puntos de montaje de datos no están bajo la raíz del punto de montaje de autofs porque el usuario raíz del host del plugin no tiene permiso para crear directorios bajo la raíz del punto de montaje de autofs.

  Si los archivos de control y de registro de recuperación se encuentran en el punto de montaje de datos, debe modificar la ruta de acceso del archivo de control y, a continuación, la ruta de acceso del archivo de registro de recuperación según corresponda.

  Puede registrar manualmente los nuevos puntos de montaje clonados con el subsistema autofs. Los puntos de montaje nuevos no se registrarán automáticamente.

- Si tiene un TDE (inicio de sesión automático) y desea clonar la base de datos en el mismo host o en otro alternativo, debe copiar la cartera (archivos de clave) en */etc/ORACLE/WALLET/$ORACLE_SID* desde la base de datos de origen a la base de datos clonada.
- Debe configurar el valor de use_lvmetad = 0 en */etc/lvm/lvm.conf* y detener el servicio lvm2-lvmetad para realizar correctamente la clonado en entornos de red de área de almacenamiento (SAN) en Oracle Linux 7 o posteriores, o Red Hat Enterprise Linux (RHEL) 7 o posteriores.
- Debe instalar el parche de Oracle 13366202 si utiliza la base de datos Oracle 11.2.0.3 o posterior y el identificador de la base de datos para la instancia auxiliar se cambia con un script NID.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup compuesto por protocolos mixtos iSCSI y FC. Para obtener más información, consulte "Error en la operación porque no puede detectar el dispositivo para la LUN".

## Clonar el backup de una base de datos de Oracle

Es posible utilizar SnapCenter para clonar una base de datos de Oracle con el backup de esa base de datos.

### Acerca de esta tarea

La operación de clonado crea una copia de los archivos de datos de la base de datos y, luego, crea nuevos archivos de registro de recuperación en línea y archivos de control. La base de datos puede recuperarse opcionalmente a una hora específica, según las opciones de recuperación especificadas.

Se produce un error en la clonado si intenta clonar un backup que se creó en un host Linux en un host AIX o viceversa.

SnapCenter crea una base de datos independiente cuando se clona desde un backup de base de datos de Oracle RAC. SnapCenter admite la creación de un clon desde el backup de bases de datos Data Guard en espera y Active Data Guard en espera.

Durante la clonado, SnapCenter monta el backup de registros para las operaciones de recuperación. Después de la recuperación, el backup de registros se desasocia. Todos estos clones están montados en */var/opt/snapcenter/scu/Clones/*. Si está usando ASM sobre NFS, debe agregar */var/opt/snapcenter/scu/clones///** a la ruta de acceso existente definida en el parámetro asm_diskstring.

Mientras se clona un backup de una base de datos ASM en un entorno SAN, se crean reglas udev para el host clonado en */etc/udev/rules.d/999-scu-netapp.rules*. Estas reglas udev asociadas con los dispositivos host clonados se eliminan cuando se elimina el clon.

En una configuración de Flex ASM, no puede realizar la operación de clonado en nodos Leaf si la cardinalidad es menor que el número de nodos del clúster RAC.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología de la base de datos.

4. En la vista Manage Copies, seleccione los backups desde local copies (primary), Mirror copies (secondary) o Vault copies (secondary).
5. Seleccione el backup de datos en la tabla y haga clic en .
6. En la página Name, realice una de las siguientes acciones:

| Si desea… | Pasos… |
| --- | --- |
| Clonar una base de datos (CDB o no CDB) | a. Especifique el SID del clon.<br><br>El SID del clon no está disponible de manera predeterminada, y la longitud máxima del SID es de 8 caracteres.<br><br>Debe asegurarse de que no exista otra base de datos con el mismo SID en el host donde se creará el clon. |
| Clonar una base de datos conectables (PDB) | a. Seleccione **PDB Clone**.<br>b. Especifique la PDB que desea clonar.<br>c. Especifique el nombre de la PDB clonada. Para ver los pasos detallados para clonar una PDB, consulte "Clonar una base de datos conectable". |

Al seleccionar un datos reflejados o de almacén:

- si no hay backup de registros en el reflejo o el almacén, no se selecciona nada y los localizadores están vacíos.
- si existen backups de registros en el reflejo o almacén, se selecciona el último backup de registros y se muestra el localizador correspondiente.

> Si el backup de registro seleccionado existe en la ubicación de reflejo y almacén, se muestran ambos localizadores.

7. En la página Locations, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Clone el host | De forma predeterminada, se completa el host de la base de datos de origen.<br><br>Si desea crear el clon en un host alternativo, seleccione el host que tiene la misma versión de Oracle y del sistema operativo que el host de la base de datos de origen. |
| Ubicaciones de los almacenes de datos | De forma predeterminada, se completa la ubicación del archivo de datos.<br><br>La convención de nomenclatura predeterminada de SnapCenter para sistemas de archivos SAN o NFS es FileSystemNameofsourcedatabase_CLONESID.<br><br>La convención de nomenclatura predeterminada de SnapCenter para grupos de discos ASM es SC_HASHCODEofDISKGROUP_CLONESID. El HASHCODEofDISKGROUP es un número generado automáticamente (entre 2 y 10 dígitos) que es único para cada grupo de discos ASM.<br><br>Si personaliza el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre respete el límite admitido por Oracle.<br><br>Si desea especificar otra ruta de acceso, debe introducir los puntos de montaje del archivo de datos o los nombres de los grupos de discos ASM para la base de datos del clon. Cuando personaliza la ruta de acceso del archivo de datos, también debe cambiar los nombres de los grupos de discos ASM del archivo de control y el archivo de registro de recuperación para que tengan el mismo nombre utilizado en los archivos de datos o cambiar el sistema de archivos a un grupo de discos ASM o sistema de archivos existente. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Archivos de control | De forma predeterminada, se completa la ruta de acceso al archivo de control.<br><br>Los archivos de control se ubican en el mismo grupo de discos ASM o sistema de archivos que los archivos de datos. Si desea anular la ruta de acceso del archivo de control, puede proporcionar otra ruta de acceso al archivo de control.<br><br>El sistema de archivos o el grupo de discos ASM deben existir en el host.<br><br>De forma predeterminada, la cantidad de archivos de control será la misma que la de la base de datos de origen. Es posible modificar la cantidad de archivos de control, pero se requiere un mínimo de un archivo de control para clonar la base de datos.<br><br>Puede personalizar la ruta de acceso del archivo de control a otro sistema de archivos (existente) distinto del de la base de datos de origen. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Rehacer registros | De forma predeterminada, se completan el grupo de archivos, la ruta de acceso y el tamaño de los archivos de registro de recuperación.<br><br>Los registros de recuperación se ubican en el mismo grupo de discos ASM o sistema de archivos que los archivos de datos de la base de datos clonada. Si desea anular la ruta de acceso del archivo de registro de recuperación, puede personalizarla en otro sistema de archivos que no sea el de la base de datos de origen.<br><br>El nuevo sistema de archivos o el grupo de discos ASM deben existir en el host.<br><br>De forma predeterminada, la cantidad de grupos de registros de recuperación, los archivos de registro de recuperación y sus tamaños serán los mismos que los de la base de datos de origen. Puede modificar los siguientes parámetros:<br><br>• Cantidad de grupos de registros de recuperación<br><br>Se requiere un mínimo de dos grupos de registros de recuperación para clonar la base de datos.<br><br>• Los archivos de registro de recuperación en cada grupo y su ruta de acceso<br><br>Puede personalizar la ruta de acceso del archivo de registro de recuperación a otro sistema de archivos (existente) distinto del de la base de datos de origen.<br><br>Se requiere un mínimo de un archivo de registro de recuperación en el grupo de registros de recuperación para clonar la base de datos.<br><br>• Tamaños del archivo del registro de recuperación |

8. En la página Credentials, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de credencial del usuario sys | Seleccione la credencial que se usará para definir la contraseña de usuario sys de la base de datos clonada.<br><br>Si SQLNET.AUTHENTICATION_SERVICES está configurado como NONE en el archivo sqlnet.ora del host de destino, no debe seleccionar **Ninguno** como la credencial en la interfaz gráfica de usuario de SnapCenter. |
| Nombre de credencial de la instancia de ASM | Seleccione **Ninguno** si está activada la autenticación del SO para conectarse a la instancia de ASM en el host del clon.<br><br>De lo contrario, seleccione la credencial de Oracle ASM configurada con el usuario "stys" o un usuario con el privilegio "sasma" aplicable al host del clon. |

El inicio, el nombre de usuario y los detalles de grupo de Oracle se completan automáticamente desde la base de datos de origen. Es posible cambiar los valores según el entorno de Oracle del host donde se creará el clon.

9. En la página PreOps, siga estos pasos:

   a. Introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de clonado.

      Debe almacenar el script previo en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script.

   b. En la sección Database Parameter settings, modifique los valores de los parámetros de la base de datos completados automáticamente que se utilizan para inicializar la base de datos.

      Para agregar parámetros adicionales, haga clic en .

      Si está utilizando Oracle Standard Edition y la base de datos se está ejecutando en el modo de registro de archivo o desea restaurar una base de datos del redo log de archivo, agregue los parámetros y especifique la ruta de acceso.

      - ARCHIVO_DE_REGISTRO_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

      > El área de recuperación rápida (FRA) no se define en los parámetros de la base de datos completados automáticamente. Para configurar la FRA, añada los parámetros relacionados.

El valor predeterminado de log_archive_dest_1 es $ORACLE_HOME/clone_sid, y los registros de archivos de la base de datos clonada se crearán en esta ubicación. Si eliminó el parámetro log_archive_dest_1, Oracle determina la ubicación del registro de archivos. Para definir una nueva ubicación para el registro de archivos, debe editar log_archive_dest_1, pero asegúrese de que el sistema de archivos o el grupo de discos existan y estén disponible en el host.

a. Haga clic en **Restablecer** para obtener la configuración predeterminada de los parámetros de la base de datos.

10. En la página PostOps, **Recover database** y **Until Cancel** se seleccionan de forma predeterminada para realizar la recuperación de la base de datos clonada.

    SnapCenter realiza la recuperación mediante el montaje del backup de registro más reciente que posee la secuencia ininterrumpida de archivos de registro después del backup de datos que se seleccionó para la clonado. El registro y el backup de datos deben estar en el almacenamiento principal para realizar la clonado en el almacenamiento principal y en el almacenamiento secundario para realizar la clonado en el almacenamiento secundario.

    Las opciones **recuperar base de datos** y **hasta Cancelar** no se seleccionan si SnapCenter no encuentra las copias de seguridad de registro adecuadas. Puede proporcionar la ubicación del archivo de registro externo si la copia de seguridad del registro no está disponible en **especificar ubicaciones de archivo de registro externo**. Se pueden especificar varias ubicaciones del registro.

    Si desea clonar una base de datos de origen configurada para admitir FRA y Oracle Managed Files (OMF), el destino del registro para la recuperación también debe respetar la estructura de directorios de OMF.

    La página PostOps no se muestra si la base de datos de origen es una base de datos Data Guard en espera o Active Data Guard en espera. Para bases de datos Data Guard en espera o Active Data Guard en espera, SnapCenter no ofrece la opción de seleccionar el tipo de recuperación en la interfaz gráfica de usuario de SnapCenter, pero la base de datos se recupera con el tipo de recuperación Until Cancel sin aplicar ningún registro.

| Nombre del campo | Descripción |
|---|---|
| Hasta Cancelar | SnapCenter realiza la recuperación mediante el montaje del backup de registro más reciente con la secuencia ininterrumpida de archivos de registro después de ese backup de datos que se seleccionó para la clonado. La base de datos clonada se recupera hasta el archivo de registro faltante o dañado. |
| Fecha y hora | SnapCenter recupera la base de datos hasta la fecha y la hora especificadas. El formato aceptado es mm/dd/yyyy hh:mm:ss<br>La hora puede especificarse en formato de 24 horas. |

| Nombre del campo | Descripción |
| --- | --- |
| Until SCN (número de cambio de sistema) | SnapCenter recupera la base de datos hasta un SCN especificado. |
| Especifique las ubicaciones de los registros de archivos externos | Especifique la ubicación del registro de archivos externo. |
| Crear nuevo DBID | De forma predeterminada **la casilla de verificación Crear nuevo DBID** está activada para generar un número único (DBID) para la base de datos clonada que lo diferencia de la base de datos de origen.<br><br>Desactive la casilla de comprobación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En esta situación, si desea registrar la base de datos clonada en el catálogo de RMAN externo donde la base de datos de origen ya está registrada, se produce un error en la operación. |
| Crear archivo temporal para tablespace temporal | Seleccione la casilla de comprobación si desea crear un archivo tempfile para el espacio de tabla temporal predeterminado de la base de datos clonada.<br><br>Si no está seleccionada la casilla de comprobación, se creará el clon de la base de datos sin el archivo tempfile. |
| Introduzca las entradas de sql que se van a aplicar al crear el clon | Agregue las entradas sql que desee aplicar al crear el clon. |
| Introduzca los scripts que se ejecutarán después de la operación de clonado | Especifique la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de clonado.<br><br>Debe almacenar el script posterior en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*.<br><br>Si colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script. |

11. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de clonado realizada, seleccione **Adjuntar informe de trabajo**.

Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Al realizar una recuperación como parte de la operación de creación de un clon, incluso si se producen errores en la recuperación, el clon se crea con una advertencia. Es posible realizar una recuperación manual de este clon para que la base de datos del clon pase a un estado consistente.

2. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**resultado**

Después de clonar la base de datos, es posible actualizar la página de recursos para que enumere la base de datos clonada como uno de los recursos disponibles para realizar backups. La base de datos clonada puede protegerse como cualquier otra base de datos con el flujo de trabajo de backup estándar, o bien puede incluirse en un grupo de recursos (recientemente creado o existente). La base de datos clonada puede volver a clonarse (clon de clones).

Después de clonar, no debe cambiar nunca el nombre de la base de datos clonada.

Si no realizó la recuperación durante la clonado, se pueden producir errores en el backup de la base de datos clonada debido a una recuperación incorrecta, y es posible que deba realizar una recuperación manual. También se pueden producir errores en el backup de registro si la ubicación predeterminada que se completó para los registros de archivos es un almacenamiento de terceros o si el sistema de almacenamiento no está configurado con SnapCenter.

En la instalación de AIX, puede utilizar el mandato lkdev para bloquear y el mandato rendev para cambiar el nombre de los discos en los que residió la base de datos clonada.

El bloqueo o cambio de nombre de dispositivos no afectará a la operación de eliminación de clones. En el caso de diseños LVM de AIX construidos en dispositivos SAN, el cambio de nombre de dispositivos no será compatible con los dispositivos SAN clonados.

**Más información**

- "La restauración o el clonado producen errores con el mensaje de error ORA-00308"
- "Error al recuperar una base de datos clonada"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

## Clonar una base de datos conectable

Es posible clonar una base de datos conectables (PDB) en una base de datos diferente o la misma CDB objetivo en el mismo host o alternativo. También es posible recuperar la PDB clonada en un SCN o la fecha y la hora que desee.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos del tipo de instancia única (Multitenant) desde la vista de detalles de la base de datos o desde la vista de detalles del grupo de recursos.

   Se muestra la página de topología de la base de datos.

4. En la vista Manage Copies, seleccione los backups desde local copies (primary), Mirror copies (secondary) o Vault copies (secondary).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Name, realice las siguientes acciones:
   a. Seleccione **PDB Clone**.
   b. Especifique la PDB que desea clonar.

      Solo es posible clonar una PDB a la vez.

   c. Especifique el nombre de la PDB del clon.
7. En la página Locations, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Clone el host | De forma predeterminada, se completa el host de la base de datos de origen.<br><br>Si desea crear el clon en un host alternativo, seleccione el host que tiene la misma versión de Oracle y del sistema operativo que el host de la base de datos de origen. |
| CDB de destino | Seleccione la CDB en el que desea incluir la PDB clonada.<br><br>Debe asegurarse de que la CDB de destino esté en ejecución. |
| Estado de la base de datos | Active la casilla de verificación **Abrir la PDB clonada en modo DE LECTURA y ESCRITURA** si desea abrir la PDB en modo DE LECTURA Y ESCRITURA. |

| | |
|---|---|
| Ubicaciones de los almacenes de datos | De forma predeterminada, se completa la ubicación del archivo de datos.<br><br>La convención de nomenclatura predeterminada de SnapCenter para sistemas DE archivos SAN o NFS es FileSystemNameofsourcedatabase_SCJOBID.<br><br>La convención de nomenclatura predeterminada de SnapCenter para grupos de discos ASM es SC_HASHCODEofDISKGROUP_SCJOBID. El HASHCODEofDISKGROUP es un número generado automáticamente (entre 2 y 10 dígitos) que es único para cada grupo de discos ASM.<br><br>Si personaliza el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre respete el límite admitido por Oracle.<br><br>Si desea especificar otra ruta de acceso, debe introducir los puntos de montaje del archivo de datos o los nombres de los grupos de discos ASM para la base de datos del clon. |

El inicio, el nombre de usuario y los detalles de grupo de Oracle se completan automáticamente desde la base de datos de origen. Es posible cambiar los valores según el entorno de Oracle del host donde se creará el clon.

8. En la página PreOps, siga estos pasos:
   a. Introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de clonado.

      Debe almacenar el script previo en /var/opt/snapcenter/spl/scripts o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso /var/opt/snapcenter/spl/scripts. Si colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script.

   b. En la sección Configuración de parámetros de la base de datos del clon auxiliar de la CDB, modifique los valores de los parámetros de la base de datos completados automáticamente que se utilizan para inicializar la base de datos.
9. Haga clic en **Restablecer** para obtener la configuración predeterminada de los parámetros de la base de datos.
10. En la página PostOps, **hasta que se selecciona Cancelar** de forma predeterminada para realizar la recuperación de la base de datos clonada.

    La opción **Until Cancel** no está seleccionada si SnapCenter no encuentra las copias de seguridad de registro adecuadas. Puede proporcionar la ubicación del archivo de registro externo si la copia de seguridad del registro no está disponible en **especificar ubicaciones de archivo de registro externo**. Se pueden especificar varias ubicaciones del registro.

Si desea clonar una base de datos de origen configurada para admitir FRA y Oracle Managed Files (OMF), el destino del registro para la recuperación también debe respetar la estructura de directorios de OMF.

| Nombre del campo | Descripción |
|---|---|
| Hasta Cancelar | SnapCenter realiza la recuperación mediante el montaje del backup de registro más reciente con la secuencia ininterrumpida de archivos de registro después de ese backup de datos que se seleccionó para la clonado.<br><br>El registro y el backup de datos deben estar en el almacenamiento principal para realizar la clonado en el almacenamiento principal y en el almacenamiento secundario para realizar la clonado en el almacenamiento secundario. La base de datos clonada se recupera hasta el archivo de registro faltante o dañado. |
| Fecha y hora | SnapCenter recupera la base de datos hasta la fecha y la hora especificadas.<br><br>La hora puede especificarse en formato de 24 horas. |
| Until SCN (número de cambio de sistema) | SnapCenter recupera la base de datos hasta un SCN especificado. |
| Especifique las ubicaciones de los registros de archivos externos | Especifique la ubicación del registro de archivos externo. |
| Crear nuevo DBID | De forma predeterminada **la casilla de verificación Crear nuevo DBID** no está seleccionada para la base de datos auxiliar de clones.<br><br>Marque la casilla de comprobación si desea generar un número único (DBID) para la base de datos clonada auxiliar que la diferencia entre la base de datos de origen. |
| Crear archivo temporal para tablespace temporal | Seleccione la casilla de comprobación si desea crear un archivo tempfile para el espacio de tabla temporal predeterminado de la base de datos clonada.<br><br>Si no está seleccionada la casilla de comprobación, se creará el clon de la base de datos sin el archivo tempfile. |

| Nombre del campo | Descripción |
| --- | --- |
| Introduzca las entradas de sql que se van a aplicar al crear el clon | Agregue las entradas sql que desee aplicar al crear el clon. |
| Introduzca los scripts que se ejecutarán después de la operación de clonado | Especifique la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de clonado.<br><br>Debe almacenar el script posterior en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso.<br><br>De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script. |

11. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

    También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de clonado realizada, seleccione **Adjuntar informe de trabajo**.

    Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.
2. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

**Después de terminar**

Si desea crear un backup de la PDB clonada, debe realizar un backup de la CDB de destino donde se clona la PDB porque no es posible realizar un backup de la PDB clonada. Debe crear una relación secundaria para la base de datos de destino para si desea crear el backup con la relación secundaria.

En una configuración de RAC, el almacenamiento para la PDB clonada solo se asocia al nodo donde se ejecutó el clon de la PDB. Las PDB de los otros nodos del RAC se encuentran en estado DE MONTAJE. Si desea que la PDB clonada sea accesible desde los otros nodos, debe asociar manualmente el almacenamiento a los otros nodos.

**Más información**

- "La restauración o el clonado producen errores con el mensaje de error ORA-00308"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

## Clonar backups de bases de datos de Oracle con comandos UNIX

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

### Acerca de esta tarea

Debe ejecutar los siguientes comandos para crear el archivo de especificación del clon de la base de datos de Oracle e iniciar la operación de clonado.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".

- Pasos*

1. Cree una especificación de clon de base de datos de Oracle a partir de una copia de seguridad especificada: *New-SmOracleCloneSpecification*

   Si la política de protección de datos secundaria es mirror-vault unificado, especifique solo -IncludeSecondaryDetails. No es necesario especificar -SecondaryStorageType.

   Este comando crea automáticamente un archivo de especificación de clon de base de datos de Oracle para la base de datos de origen especificada y su backup. Además debe proporcionar un SID de base de datos del clon para que el archivo de especificación creado tenga los valores generados automáticamente para la base de datos del clon que creará.

   El archivo de especificación del clon se crea en */var/opt/snapcenter/sco/clone_specs*.

2. Inicie una operación de clonado desde un grupo de recursos de clon o un backup existente: *New-SmClone*

   Este comando inicia una operación de clonado. También debe proporcionar una ruta de acceso al archivo de especificación del clon de Oracle para la operación de clonado. Además, puede especificar las opciones de recuperación, el host donde se realizará la operación de clonado, scripts previos, scripts posteriores y otros detalles.

De forma predeterminada, el archivo de destino del registro de archivos para la base de datos del clon se completa automáticamente en *$ORACLE_HOME/CLONE_SIDS*.

## Divida el clon de una base de datos de Oracle

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

### Acerca de esta tarea

- No se puede ejecutar la operación de división de clones en un clon intermedio.

  Por ejemplo, después de crear el clon 1 a partir de un backup de la base de datos, puede realizar un backup del clon 1 y luego clonar este backup (que sería el clon 2). Una vez creado el clon 2, el clon 1 se convierte en un clon intermedio y la operación de división de clones puede hacerse con el clon 1. No obstante, esta operación también puede ejecutarse con el clon 2.

Después de dividir el clon 2, puede ejecutar la operación de división de clones con el clon 1, ya que este deja de ser el clon intermedio.

- Cuando divide un clon, se eliminan las copias del backup del clon.
- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Asegúrese de que el volumen o el agregado del sistema de almacenamiento estén en línea.
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Database** en la lista **View**.
3. Seleccione el recurso clonado (por ejemplo, la base de datos o el LUN) y haga clic en .
4. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

   La operación de división de clones se detiene si se reinicia el servicio SMCore y las bases de datos en las que se ejecutó la operación de división de clones aparecen como clones en la página Resources. Debe ejecutar el cmdlet *Stop-SmJob* para detener la operación de división de clones y luego volver a intentar la operación de división de clones.

   Si necesita más o menos tiempo de sondeo para comprobar si el clon está dividido o no, puede cambiar el valor del parámetro CloneSplitStatusCheckPollTime en el archivo SMCoreServiceHost.exe.config. De este modo, se establece un intervalo para que SMCore sondee el estado de la operación de división de clones. El valor se registra en milisegundos; el predeterminado son 5 minutos.

   Por ejemplo:

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

Se produce un error en la operación de inicio de división de clones si hay un backup, una restauración o una división de clones en curso. Solo debe reiniciar la operación de división de clones una vez que hayan finalizado las operaciones en ejecución.

## Clon dividido de una base de datos conectable

Es posible utilizar SnapCenter para dividir una base de datos conectables (PDB) clonada.

### Acerca de esta tarea

Si creó un backup de la CDB de destino donde se clona la PDB, al dividir la PDB, la PDB clonada también se quita de todos los backups de la CDB de destino que contiene la PDB clonada.

Los clones de las PDB no se muestran en la vista de inventario o recursos.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Seleccione la base de datos del contenedor de origen (CDB) en la vista del recurso o grupo de recursos.
  3. En la vista Manage Copies (Administrar copias), seleccione **Clones** ya sea en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
  4. Seleccione el clon de la PDB (targetCDB:PDBClone) y, a continuación, haga clic en .
  5. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
  6. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Supervise las operaciones de clonado de las bases de datos de Oracle

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **trabajos**, realice los siguientes pasos:
     a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
     b. Especifique las fechas de inicio y finalización.
     c. En la lista desplegable **Tipo**, seleccione **Clonar**.
     d. En la lista desplegable **Estado**, seleccione el estado del clon.
     e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
  4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Actualizar un clon

Para actualizar el clon, puede ejecutar el comando *Refresh-SmClone*. Este comando crea un backup de la base de datos, elimina el clon existente y crea un clon con el mismo nombre.

No se puede actualizar un clon de una PDB.

**Lo que necesitará**

- Cree un backup completo en línea o una política de backup de datos sin conexión sin conexión sin backups programados habilitados.
- Configure la notificación por correo electrónico en la directiva sólo para los fallos de copia de seguridad.
- Defina el número de retención de los backups bajo demanda correctamente para garantizar que no haya backups no deseados.
- Asegúrese de que solo exista asociada una política de backup completo en línea o de backup de datos sin conexión a un grupo de recursos identificado para la operación de actualización de clonado.
- Cree un grupo de recursos con solo una base de datos.
- Si se crea un trabajo de cron para el comando clone Refresh, asegúrese de que las programaciones de SnapCenter y de cron no se superpongan para el grupo de recursos de la base de datos.

  Para un trabajo de cron creado para el comando clone Refresh, asegúrese de ejecutar Open-SmConnection cada 24 horas.

- Asegúrese de que el SID del clon sea único para un host.

  Si diversas operaciones de clonado de actualización utilizan el mismo archivo de especificación de clon o utilizan el archivo de especificación de clon con el mismo SID de clon, se eliminará el clon existente con el SID del host y, a continuación, se creará el clon.

- Asegúrese de que la política de backup esté habilitada con protección secundaria y que el archivo de especificación del clon se cree con "'-IncludeSecondaryDetails" para crear los clones con backups secundarios.
  - Si se especifica el archivo de especificación del clon principal pero la política tiene seleccionada la opción de actualización secundaria, se creará el backup y la actualización se transferirá al secundario. Sin embargo, el clon se creará a partir del backup primario.
  - Si se especifica el archivo de especificación del clon principal y la política no tiene seleccionada la opción de actualización secundaria, se creará el backup en la ubicación principal y se creará el clon a partir de la ubicación principal.
- Pasos*

1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado: *Open-SmConnection*
2. Cree una especificación de clon de base de datos de Oracle a partir de una copia de seguridad especificada: *New-SmOracleCloneSpecification*

   Si la política de protección de datos secundaria es mirror-vault unificado, especifique solo -IncludeSecondaryDetails. No es necesario especificar -SecondaryStorageType.

Este comando crea automáticamente un archivo de especificación de clon de base de datos de Oracle para la base de datos de origen especificada y su backup. Además debe proporcionar un SID de base de datos del clon para que el archivo de especificación creado tenga los valores generados automáticamente para la base de datos del clon que creará.

> El archivo de especificación del clon se crea en */var/opt/snapcenter/sco/clone_specs*.

3. Ejecute *Refresh-SmClone*.

   Si la operación falla con los mensajes de error "PL-SCO-20032: CanExecute operación falló con el error: PL-SCO-30031: Redo log file +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists", especifique un valor superior para *-WaitToTriggerClone*.

Para obtener información detallada sobre comandos UNIX, consulte "Guía de referencia de comandos del software SnapCenter".

## Eliminar el clon de una base de datos conectables

Es posible eliminar el clon de una base de datos conectables (PDB) si ya no se necesita.

Si creó un backup de la CDB de destino donde se clona la PDB, al eliminar la clonado de la PDB, la PDB clonada también se quita del backup de la CDB de destino.

> Los clones de las PDB no se muestran en la vista de inventario o recursos.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. Seleccione la base de datos del contenedor de origen (CDB) en la vista del recurso o grupo de recursos.
3. En la vista Manage Copies (Administrar copias), seleccione **Clones** ya sea en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
4. Seleccione el clon de la PDB (targetCDB:PDBClone) y, a continuación, haga clic en .
5. Haga clic en **Aceptar**.

# Protección de sistemas de archivos Windows

## Conceptos del plugin de SnapCenter para Microsoft Windows

### Información general sobre el plugin de SnapCenter para Microsoft Windows

El plugin de SnapCenter para Microsoft Windows es un componente en el lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de recursos de sistemas de archivos Microsoft. Además, ofrece aprovisionamiento de almacenamiento, consistencia de copias de Snapshot y reclamación de espacio para sistemas de archivos Windows. El plugin para Windows automatiza las operaciones de backup, restauración y clonado del sistema de archivos en el entorno de SnapCenter.

Cuando se instala el plugin para Windows, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear copias de reflejo de conjuntos de backups en otro volumen, y también con la tecnología SnapVault de NetApp para realizar replicaciones de backup disco a disco para archivado o cumplimiento de normativas.

### Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft Windows

Cuando el plugin para Windows está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar sistemas de archivos Windows. También es posible ejecutar tareas complementarias a estas operaciones.

- Detectar recursos
- Realizar backup de sistemas de archivos Windows
- Programar operaciones de backup
- Restaurar backups de sistema de archivos
- Clonar backups de sistema de archivos
- Supervisar operaciones de backup, de restauración y de clonado

El plugin para Windows no es compatible con el backup y la restauración de sistemas de archivos en los recursos compartidos SMB.

### Funciones del plugin de SnapCenter para Windows

El plugin para Windows se integra con la tecnología de copia de Snapshot de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para Windows, se utiliza la interfaz de SnapCenter.

El plugin para Windows incluye estas características principales:

- **Interfaz gráfica de usuario unificada con tecnología SnapCenter**

La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar procesos de backup y restauración consistentes entre plugins, utilizar informes centralizados, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins. SnapCenter además ofrece gestión de políticas y programación centralizada para admitir operaciones de backup y clonado.

- **Administración central automatizada**

  Es posible programar backups del sistema de archivos rutinarios, configurar retención de backups basada en políticas y configurar operaciones de restauración. Si desea supervisar de manera proactiva el entorno del sistema de archivos, configure SnapCenter para que envíe alertas por correo electrónico.

- **Tecnología de copia snapshot de NetApp** no disruptiva

  El plugin para Windows utiliza la tecnología de copia de Snapshot de NetApp. Esto permite realizar backups de sistemas de archivos en cuestión de segundos y restaurarlos rápidamente sin necesidad de dejar sin conexión el host. Las copias de Snapshot consumen un espacio de almacenamiento mínimo.

Además de estas funciones principales, el plugin para Windows ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración y clonado
- Seguridad compatible con RBAC y delegación de roles centralizada
- Creación de copias de sistemas de archivos de producción con gestión eficiente del espacio para realizar pruebas o extraer datos con la tecnología FlexClone de NetApp

  Para obtener información sobre la licencia de FlexClone, consulte "Licencias SnapCenter".

- Capacidad para ejecutar varios backups al mismo tiempo entre varios servidores
- Cmdlets de PowerShell para crear scripts de operaciones de backup, restauración y clonado
- Compatibilidad con backup de sistemas de archivos y VMDK
- Compatibilidad con infraestructuras físicas y virtualizadas
- Compatibilidad con iSCSI, Fibre Channel, FCoE, RDM, ALM, VMDK sobre NFS y VMFS, y FC virtual

## Cómo hace SnapCenter para realizar backup de sistemas de archivos Windows

SnapCenter usa la tecnología de copia de Snapshot para realizar backups de los recursos del sistema de archivos Windows que residen en LUN, CSV (volúmenes compartidos de clúster), volúmenes RDM, ALM en clústeres de Windows y VMDK basado en VMFS/NFS (sistema de archivos de máquina virtual VMware con NFS).

SnapCenter crea backups a partir de copias snapshot de los sistemas de archivos. Los backups federados, en los que un mismo volumen contiene LUN de varios hosts, son más rápidos y eficientes que los backups de cada LUN individual porque solo se crea una copia de Snapshot del volumen, en lugar de Snapshots individuales de cada sistema de archivos.

Cuando SnapCenter crea una copia de Snapshot, se captura todo el volumen del sistema de almacenamiento en la copia de Snapshot. Sin embargo, el backup solo es válido para el servidor de host para el cual se creó el backup.

Si hay datos de otros servidores de host en el mismo volumen, no es posible restaurarlos desde la copia de Snapshot.

Si un sistema de archivos Windows contiene una base de datos, el proceso de backup del sistema de archivos no es igual que el de la base de datos. Para realizar un backup de una base de datos, se usa uno de los plugins de la base de datos.

## Tipos de almacenamiento compatibles con los plugins de SnapCenter para Microsoft Windows

SnapCenter es compatible con una gran variedad de tipos de almacenamiento, tanto en máquinas físicas como virtuales. Antes de instalar el paquete para el host, es necesario verificar que el tipo de almacenamiento sea compatible.

Windows Server es compatible con el aprovisionamiento y la protección de datos de SnapCenter. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
|---|---|---|---|
| Servidor físico | LUN conectados a FC | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Servidor físico | LUN conectados a iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Servidor físico | Recursos compartidos de SMB3 (CIFS) que residen en una máquina virtual de almacenamiento (SVM) | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Compatibilidad solo para aprovisionamiento.<br><br>No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB. |
| Máquina virtual de VMware | LUN de RDM conectados por un adaptador de bus de host FC o iSCSI | Cmdlets de PowerShell | |
| Máquina virtual de VMware | LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Máquina virtual de VMware | Sistemas de archivos de máquina virtual (VMFS) o almacenes de datos NFS | VSphere de VMware | |

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
| --- | --- | --- | --- |
| Máquina virtual de VMware | Un sistema invitado conectado a recursos compartidos de SMB3 que residen en una SVM | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Compatibilidad solo para aprovisionamiento.<br><br>No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB. |
| Máquina virtual Hyper-V. | LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Para aprovisionar LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual se debe usar Hyper-V Manager.<br><br>No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |
| Máquina virtual Hyper-V. | LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
| --- | --- | --- | --- |
| Máquina virtual Hyper-V. | Un sistema invitado conectado a recursos compartidos de SMB3 que residen en una SVM | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Compatibilidad solo para aprovisionamiento.<br><br>No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB.<br><br>No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |

## Privilegios mínimos de ONTAP requeridos para el plugin de Windows

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| event generate-autosupport-log |
| se muestra el historial del trabajo<br><br>detención de trabajo |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| lun |
| lun create |
| eliminación de lun |
| igroup de lun añadido |
| crear lun igroup |
| lun igroup eliminado |
| cambio de nombre de lun igroup |
| lun igroup show |
| asignación de lun de nodos adicionales |
| se crea la asignación de lun |
| se elimina la asignación de lun |
| asignación de lun quitar nodos de generación de informes |
| se muestra el mapa de lun |
| modificación de lun |
| movimiento de lun en volumen |
| lun desconectada |
| lun conectada |
| cambio de tamaño de lun |
| serie de lun |
| muestra de lun |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| regla adicional de la política de snapmirror<br>regla de modificación de la política de snapmirror<br>regla de eliminación de la política de snapmirror<br>la política de snapmirror<br>restauración de snapmirror<br>de snapmirror<br>historial de snapmirror<br>actualización de snapmirror<br>conjunto de actualizaciones de snapmirror<br>destinos de listas de snapmirror |
| versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| crear el clon de volumen |
| show de clon de volumen |
| inicio de división de clon de volumen |
| detención de división de clon de volumen |
| cree el volumen |
| destrucción del volumen |
| crear el archivo de volumen |
| uso show-disk del archivo de volumen |
| volumen sin conexión |
| volumen en línea |
| modificación del volumen |
| crear el qtree de volúmenes |
| eliminación de qtree de volumen |
| modificación del qtree del volumen |
| se muestra volume qtree |
| restricción de volumen |
| visualización de volumen |
| crear snapshots de volumen |
| eliminación de snapshots de volumen |
| modificación de las copias de snapshot de volumen |
| cambio de nombre de copias de snapshot de volumen |
| restauración de copias snapshot de volumen |
| archivo de restauración de snapshots de volumen |
| visualización de copias de snapshot de volumen |
| desmonte el volumen |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| vserver cifs |
| vserver cifs share create |
| eliminación de vserver cifs share |
| se muestra vserver shadowcopy |
| visualización de vserver cifs share |
| visualización de vserver cifs |
| política de exportación de vserver |
| creación de política de exportación de vserver |
| eliminación de la política de exportación de vserver |
| creación de reglas de política de exportación de vserver |
| aparece la regla de política de exportación de vserver |
| visualización de la política de exportación de vserver |
| vserver iscsi |
| se muestra la conexión iscsi del vserver |
| se muestra vserver |

| Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| interfaz de red |
| se muestra la interfaz de red |
| vserver |

## Preparar los sistemas de almacenamiento para la replicación con SnapMirror y SnapVault

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en

el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

> SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

## Defina una estrategia de backup para sistemas de archivos de Windows

Definir una estrategia de backup antes de crear backups garantiza que se cuente con todos los backups necesarios para restaurar o clonar correctamente los sistemas de archivos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

### Programaciones de backup para sistemas de archivos Windows

La frecuencia de los backups se especifica en las políticas; la programación de los backups se especifica en la configuración del grupo de recursos. El factor más crítico para determinar la frecuencia o la programación de los backups es la tasa de cambio del recurso y la importancia de los datos. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores son la importancia del recurso para la organización, el SLA y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso en el caso de un recurso utilizado intensivamente, no existe el requisito de ejecutar un backup completo más de una o dos veces al día.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de los backups (cada cuánto tiempo deben realizarse los backups), denominada *schedule type* para algunos plugins, forma parte de la configuración de una política. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual, o puede especificar **Ninguno** que convierte la política en una directiva sólo bajo demanda. Puede acceder a las directivas haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

Las programaciones de los backups (el momento exacto en que se realizan los backups) forman parte de una configuración de grupo de recursos. Por ejemplo, si tiene un grupo de recursos que posee una política configurada para backups semanales, quizás sea conveniente configurar la programación para que realice backups todos los jueves a las 00:10. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **grupos de recursos**.

### Cantidad de tareas de backup necesarias para sistemas de archivos Windows

Algunos factores que determinan la cantidad de backups que se necesitan son el tamaño del sistema de archivos Windows, la cantidad de volúmenes que se usan, la tasa de cambio del recurso y el acuerdo de nivel de servicio.

### Convención de nomenclatura de backups para sistemas de archivos Windows

Los backups del sistema de archivos Windows usan la convención de nomenclatura predeterminada para las copias de Snapshot. La convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de las copias de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La copia de Snapshot usa la siguiente convención de nomenclatura predeterminada: Resourcegroupname_hostname_timestamp

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- `dts1` es el nombre del grupo de recursos.
- `mach1x88` es el nombre del host.
- `03-12-2016_23.17.26` es la fecha y la marca de hora.

Al crear un backup, también se puede añadir una etiqueta descriptiva que ayude a identificar el backup. Por el contrario, si se desea usar una convención de nomenclatura de backup personalizada, se debe cambiar el nombre del backup una vez que finaliza la operación de backup.

### Opciones de retención de backups

Es posible elegir la cantidad de días durante los cuales se retendrán las copias de backup o especificar la cantidad de copias de backup que se desean retener, con un máximo de 255 copias en ONTAP. Por ejemplo, una organización puede necesitar retener 10 días de copias de backup o 130 copias de backup.

Al crear una política, es posible especificar las opciones de retención para cada tipo y programación de backup.

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

SnapCenter elimina los backups previos que tengan etiquetas de retención que coincidan con el tipo de programación. Si se modifica el tipo de programación para el recurso o el grupo de recursos, los backups con la etiqueta del tipo de programación anterior podrían conservarse en el sistema.

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

### Orígenes y destinos de clones para sistemas de archivos Windows

Es posible clonar un backup del sistema de archivos desde un almacenamiento primario o almacenamiento secundario. También puede elegir un destino compatible con sus requisitos, que puede ser la ubicación del backup original u otro destino en el mismo host o en otro. El destino debe estar en el mismo volumen que el backup de origen clonado.

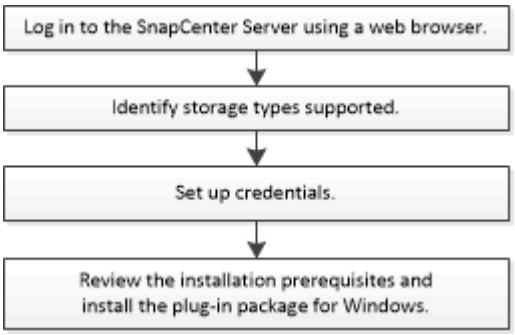
| Destino de clones | Descripción |
|---|---|
| Original, origen, ubicación | De forma predeterminada, SnapCenter almacena el clon en la misma ubicación y el mismo host que el backup que se clona. |
| Otra ubicación | Es posible almacenar el clon en otra ubicación en el mismo host o en otro. El host debe tener una conexión configurada a la SVM. |

Se puede cambiar el nombre del clon cuando finaliza la operación de clonado.

# Instale el plugin de SnapCenter para Microsoft Windows

### Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Windows

Debe instalar y configurar el plugin de SnapCenter para Microsoft Windows si desea proteger los archivos de Windows que no sean archivos de base de datos.




### Requisitos de instalación del plugin de SnapCenter para Microsoft Windows

Debe estar al tanto de determinados requisitos de instalación antes de instalar el plugin para Windows.

Antes de empezar a utilizar el plugin para Windows, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas de requisitos previos.

- Debe tener privilegios de administrador de SnapCenter para instalar el plugin para Windows.

La función de administrador de SnapCenter debe tener privilegios de administración.

- Debe haber instalado y configurado el servidor SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Debe configurar SnapMirror y SnapVault si desea una replicación de backup.

### Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows

Antes de instalar el paquete de plugins de SnapCenter para Windows, debe estar familiarizado con algunos requisitos básicos de espacio y tamaño del sistema host.

| Elemento | Requisitos |
|---|---|
| Sistemas operativos | Microsoft Windows<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 5 GB<br><br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |
| Paquetes de software obligatorios | • Microsoft .NET Framework 4.5.2 o posterior<br>• Windows Management Framework (WMF) 4.0 o posterior<br>• PowerShell 4.0 o posterior<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |

### Configure sus credenciales para el plugin para Windows

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar los plugins de SnapCenter, y credenciales adicionales para realizar operaciones de protección de datos en sistemas de archivos Windows.

**Lo que necesitará**

- Debe configurar credenciales de Windows antes de instalar plugins.
- Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador, en el host remoto.
- Si se configuran credenciales para grupos de recursos individuales y el usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al usuario.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Settings, haga clic en **Credential**.
  3. Haga clic en **Nuevo**.
  4. En la página Credential, haga lo siguiente:

| **Para este campo…** | **Realice lo siguiente…** |
| --- | --- |
| Nombre de credencial | Introduzca un nombre para las credenciales. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario/Contraseña | Introduzca el nombre de usuario y la contraseña para la autenticación.<br>• Administrador de dominio o cualquier miembro del grupo de administradores<br>Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Username son los siguientes:<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>◦ `UserName@upn`<br>• Administrador local (sólo para grupos de trabajo)<br>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es el siguiente: `UserName`<br>No utilice comillas dobles (") ni marcas de retroceso (') en las contraseñas. No debe usar el signo menos de (<) y el signo de exclamación (!) los símbolos juntos en las contraseñas. Por ejemplo, arrendhan<!10, les10<!, backtick'12. |
| Contraseña | Introduzca la contraseña usada para autenticación. |

5. Haga clic en **Aceptar**.

   Después de terminar de configurar las credenciales, es posible que desee asignar mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

### Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio

administrado.

**Lo que necesitará**

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

1. Asigne los privilegios administrativos al GMSA configurado en el host.
2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

   El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

## Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

**Lo que necesitará**

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

      Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. Reinicie el host.
   b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
   c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`
      1. Asigne los privilegios administrativos al GMSA configurado en el host.
      2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

## Añada hosts e instale el plugin de SnapCenter para Microsoft Windows

Puede utilizar la página SnapCenter Add Host para añadir hosts de Windows. El plugin de SnapCenter para Microsoft Windows está instalado automáticamente en el host especificado. Este es el método recomendado para la instalación de plugins. Puede añadir un host e instalar un plugin para un host individual o para un clúster.

**Lo que necesitará**

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- El usuario de SnapCenter debe agregarse a la función «'Iniciar sesión como servicio'» del servidor Windows.
- Debe asegurarse de que el servicio de cola de mensajes esté en estado en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configurar la cuenta de servicio administrado de grupo en Windows Server 2012 o posterior para el sistema de archivos de Windows"

**Acerca de esta tarea**

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Plugins de Windows
  - Microsoft Windows
  - Servidor de Microsoft Exchange
  - Microsoft SQL Server
  - SAP HANA
  - Plugins personalizados
- Instalar plugins en un clúster

  Si instala plugins en un clúster (WSFC, Oracle RAC o DAG de Exchange), se instalan en todos los nodos del clúster.

- Almacenamiento E-series

  No puede instalar el plugin para Windows en un host de Windows conectado al almacenamiento E-series.

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. Asegúrese de que **Managed hosts** esté seleccionado en la parte superior.

3. Haga clic en **Agregar**.
4. En la página hosts, realice lo siguiente:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de host | Seleccione el tipo de host **Windows**.<br><br>El servidor de SnapCenter añade el host y, a continuación, instala el plugin para Windows si aún no está instalado en el host. |
| Nombre de host | Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.<br><br>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el nombre de dominio completamente cualificado (FQDN).<br><br>Puede introducir las direcciones IP o el FQDN de uno de los siguientes:<br><br>• Host independiente<br>• Clustering de conmutación al nodo de respaldo de Windows Server (WSFC)<br><br>Si va a añadir un host mediante SnapCenter y forma parte de un subdominio, debe proporcionar el FQDN. |
| Credenciales | Seleccione el nombre de credencial que ha creado o cree las credenciales nuevas.<br><br>Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte los detalles de cómo crear una credencial.<br><br>Los detalles sobre las credenciales, incluidos el nombre de usuario, el dominio y el tipo de host, se muestran colocando el cursor sobre el nombre de las credenciales que ha proporcionado.<br><br>El modo de autenticación se determina por el tipo de host que especifique en el asistente Add host. |

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.

   Para nuevas implementaciones, no aparece ningún paquete de plugins.

6. (Opcional) haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto.<br><br>El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. |
| Ruta de instalación | La ruta predeterminada es C:\Program Files\NetApp\SnapCenter.<br><br>Opcionalmente, puede personalizar la ruta. Para el paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Sin embargo, si lo desea, puede personalizar la ruta predeterminada. |
| Añada todos los hosts del clúster | Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un WSFC. |
| Omitir comprobaciones previas a la instalación | Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin. |
| Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in | Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de complemento.<br><br>Proporcione el nombre de GMSA con el siguiente formato: *Domainname\accountName$*.<br><br>GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows. |

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla de comprobación **Skip prechecks**, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. Se comprueban el espacio en disco, la memoria RAM, la versión de PowerShell, la versión de NET y la ubicación comparando estos elementos con los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

Si el error está relacionado con el espacio en disco o la RAM, puede actualizar el archivo web.config ubicado en `C:\Program Files\NetApp\SnapCenter` Webapp para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero debe solucionar el problema.

En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

1. Supervise el progreso de la instalación.

## Instale el plugin de SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell

Si desea instalar el plugin de SnapCenter para Microsoft Windows en varios hosts a la vez, puede hacerlo mediante el `Install-SmHostPackage` Cmdlet de PowerShell.

Tiene que haber iniciado sesión en SnapCenter como usuario del dominio con derechos de administrador local en cada host en el que desee instalar los plugins.

- Pasos*
  1. Inicie PowerShell.
  2. En el host del servidor SnapCenter, establezca una sesión mediante el `Open-SmConnection` cmdlet y, a continuación, introduzca las credenciales.
  3. Añada el host o el clúster independiente a SnapCenter mediante el `Add-SmHost` cmdlet y los parámetros necesarios.

     La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

  4. Instale el plugin en varios hosts mediante el `Install-SmHostPackage` cmdlet y los parámetros necesarios.

     Puede utilizar el `-skipprecheck` opción cuando instaló los plugins manualmente y no desea validar si el host cumple con los requisitos para instalar el plugin.

## Instale el plugin de SnapCenter para Microsoft Windows silenciosamente desde la línea de comandos

Puede instalar el plugin de SnapCenter para Microsoft Windows localmente en un host de Windows si no puede instalar el plugin de forma remota desde la interfaz gráfica de usuario de SnapCenter. Puede ejecutar el programa de instalación del plugin de SnapCenter para Microsoft Windows sin supervisión y en el modo silencioso desde la línea de comandos de Windows.

**Lo que necesitará**

- Debe haber instalado Microsoft.Net 4.5.2 o superior.
- Debe haber instalado PowerShell 4.0 o posterior.
- Debe haber activado la cola de mensajes de Windows.
- Debe ser un administrador local en el host.
- Pasos*

1. Descargue el plugin de SnapCenter para Microsoft Windows desde su ubicación de instalación.

   Por ejemplo, la ruta de instalación predeterminada es C:\ProgramData\NetApp\SnapCenter\Package Repository.

   Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

2. Copie el archivo de instalación en el host en el que desea instalar el plugin.
3. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación.
4. Introduzca el siguiente comando y sustituya las variables por sus datos:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Por ejemplo:

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Todos los parámetros que se pasan durante la instalación del plugin para Windows distinguen entre mayúsculas y minúsculas.

   Introduzca los valores para las siguientes variables:

| Variable | Valor |
|---|---|
| */DEBUGLOG"<Debug_Log_Path>* | Especifique el nombre y la ubicación del archivo de registro del instalador del paquete, como en el ejemplo siguiente: setup.exe /DEBUGLOG"C:\PathToLog\setupexe.log". |
| BI_SNAPCENTER_PORT | Indique el puerto en el que SnapCenter se comunica con SMCore. |

| Variable | Valor |
| --- | --- |
| SUITE_INSTALLDIR | Indique el directorio de instalación para el paquete de plugins del host. |
| BI_SERVICEACCOUNT | Indique la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows. |
| BI_SERVICEPWD | Indique la contraseña para la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows. |
| ISFeatureInstall | Indique la solución que debe aplicar SnapCenter en un host remoto. |

El parámetro *DEBUGLOG* incluye la ruta del archivo de registro para SnapCenter. Escribir en este archivo de registro es el método preferido para obtener información de resolución de averías, ya que el archivo contiene los resultados de las comprobaciones que se realizan durante la instalación con respecto a los requisitos del plugin.

Si es necesario, puede encontrar más información sobre la solución de problemas en el archivo de registro del paquete SnapCenter para Windows. Los archivos de registro del paquete se muestran (los más antiguos primero) en la carpeta *%Temp%*, por ejemplo, *C:\temp*.

La instalación del plugin para Windows registra el plugin en el host, no en el servidor de SnapCenter. Es posible registrar el plugin en SnapCenter Server. Para ello, se debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Una vez añadido el host, el plugin se detecta automáticamente.

## Supervise el estado de instalación del paquete de plugins de SnapCenter

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

**Acerca de esta tarea**

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.

2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
   a. Haga clic en **filtro**.
   b. Opcional: Indique las fechas de inicio y finalización.
   c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
   d. En el menú desplegable de estado, seleccione el estado de instalación.
   e. Haga clic en **aplicar**.
4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configure el certificado de CA

### Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

> Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

### Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

- Pasos*
  1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
  2. En la ventana **Agregar o quitar complementos**, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
  3. En la ventana del complemento **certificados**, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
  4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.

5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
|---|---|
| Importar clave privada | Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**. |
| Importar formato de archivo | No realice cambios; haga clic en **Siguiente**. |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |
| Finalización del Asistente para importación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación. |

> El certificado de importación debe incluirse con la clave privada (los formatos admitidos son: *.pfx, *.p12, *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

**Obtenga la huella digital del certificado de CA**

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

- Pasos*
  1. Realice lo siguiente en la interfaz gráfica de usuario:
     a. Haga doble clic en el certificado.
     b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
     c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
     d. Copie los caracteres hexadecimales del cuadro.
     e. Quite los espacios entre los números hexadecimales.

        Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

  2. Realice lo siguiente desde PowerShell:
     a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

        *Get-ChildItem -Path Cert:\LocalMachine\My*

     b. Copie la huella digital.

### Configure el certificado de CA con servicios de plugins de host de Windows

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

- Pasos*

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

   Por ejemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Enlace el certificado recientemente instalado con los servicios de plugins del host de Windows mediante la ejecución de los siguientes comandos:
   ```

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert appid="$guid"
   ```

   Por ejemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
```

### Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

### Lo que necesitará

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

**Después de terminar**

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

# Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

## Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

## Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

# Realizar backup de sistemas de archivos Windows

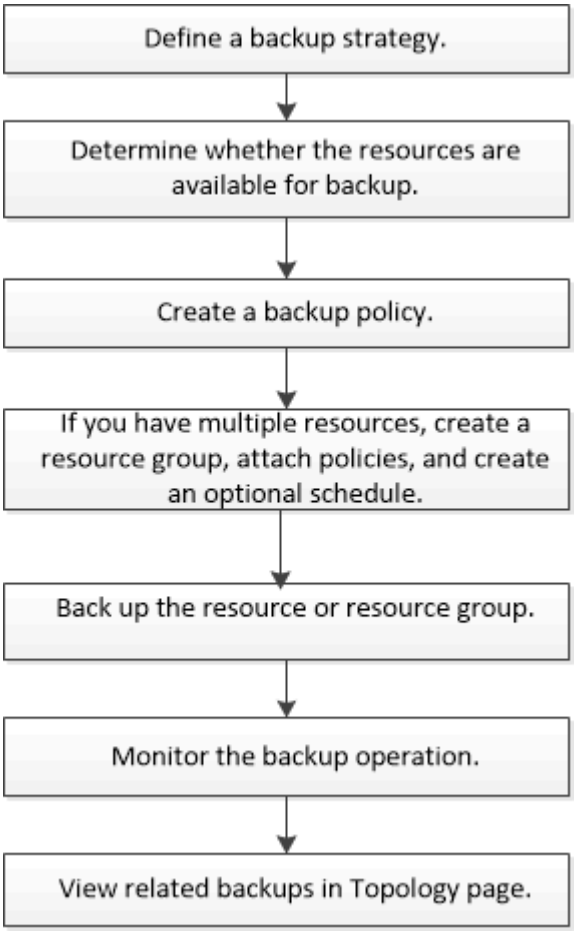
## Realizar backup de sistemas de archivos Windows

Al instalar el plugin de SnapCenter para Microsoft Windows en el entorno, puede utilizar

SnapCenter para realizar backups de sistemas de archivos Windows. Puede realizar el backup de un solo sistema de archivos o de un grupo de recursos que contenga varios sistemas de archivos. Es posible realizar un backup bajo demanda o según una programación de protección definida.

Es posible programar varios backups para que se realicen simultáneamente en diferentes servidores. No se pueden ejecutar en simultáneo operaciones de backup y restauración en el mismo recurso.

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de backup:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda de cmdlet de SnapCenter o la "Guía de referencia de cmdlets de SnapCenter Software" Contiene información detallada sobre los cmdlets de PowerShell.

## Determinar la disponibilidad de recursos para los sistemas de archivos Windows

Los recursos son los LUN y componentes similares del sistema de archivos que se mantienen mediante los plugins instalados. Puede añadir esos recursos a grupos de recursos para que pueda realizar trabajos de protección de datos en múltiples recursos, pero primero debe identificar qué recursos tiene disponible. Al detectar los recursos disponibles también se verifica que la instalación de plugins se realizó correctamente.

**Lo que necesitará**

- Ya debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts, crear conexiones de máquina virtual de almacenamiento (SVM) y añadir credenciales.
- Si los archivos residen en LUN o VMDK de VMware, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin en SnapCenter. Para obtener más información, consulte "Documentación del plugin de SnapCenter para VMware vSphere".
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **File Systems** en la lista.
  3. Seleccione el host para filtrar la lista de recursos y, a continuación, haga clic en **Actualizar recursos**.

     Los sistemas de archivos agregados, cuyo nombre se ha cambiado o eliminado recientemente se actualizan al inventario de SnapCenter Server.

## Crear políticas de backup para sistemas de archivos Windows

Puede crear una nueva política de backup para recursos antes de usar SnapCenter para realizar backups de sistemas de archivos Windows, o bien puede crear una nueva política de backup en el momento de crear un grupo de recursos o al realizar el backup de un recurso.

**Lo que necesitará**

- Debe tener definida una estrategia de backup. "Leer más"
- Debe tener preparada la protección de datos.

  Para prepararse para la protección de datos, debe completar ciertas tareas, como instalar SnapCenter, añadir hosts, detectar recursos y crear conexiones de máquina virtual de almacenamiento (SVM).
- Si desea replicar copias de Snapshot en un almacenamiento secundario con SnapMirror o SnapVault, el administrador de SnapCenter debe haberle asignado las SVM de los volúmenes de origen y de destino.
- Si desea ejecutar los scripts de PowerShell en scripts previos y posteriores, debe establecer el valor del parámetro usePowershellProcessforScripts en TRUE en el archivo web.config.

  El valor predeterminado es FALSE
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Directivas**.
  3. Para determinar si puede utilizar una directiva existente, seleccione el nombre de la directiva y, a continuación, haga clic en **Detalles**.

     Después de revisar las políticas existentes, puede realizar una de las siguientes acciones:

     - Usar una política existente.
     - Copiar una política existente y modificar su configuración.
     - Crear una nueva política.

4. Para crear una nueva directiva, haga clic en **Nuevo**.
5. En la página Name, introduzca el nombre de la política y una descripción.
6. En la página Backup Options, realice las siguientes tareas:

   a. Seleccione un valor para backup.

| Opción | Descripción |
|---|---|
| Copia de seguridad consistente del sistema de archivos | Elija esta opción si desea que SnapCenter ponga en modo inactivo la unidad de disco en la que reside el sistema de archivos antes de que comience la operación de backup y luego la reanude tras finalizar dicha operación. |
| Copia de seguridad coherente con los fallos del sistema de archivos | Elija esta opción si no desea que SnapCenter ponga en modo inactivo la unidad de disco en la que reside el sistema de archivos. |

   b. Seleccione una frecuencia de programación (también llamada tipo de política).

      La política especifica solamente la frecuencia de backup. La programación de protección específica para realizar el backup se define en el grupo de recursos. Por lo tanto, dos o más grupos de recursos pueden compartir la misma política y frecuencia de backup y, a su vez, tener diferentes programaciones de backup.

      Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

7. En la página Retention, especifique la configuración de retención para backups bajo demanda y para cada frecuencia de programación que seleccionó.

| Opción | Descripción |
|---|---|
| Total de copias de Snapshot que se conservan | Elija esta opción si desea especificar el número de copias de Snapshot que almacena SnapCenter antes de eliminarlas automáticamente. |
| Elimine las copias Snapshot con antigüedad superior a | Elija esta opción si desea especificar el número de días que SnapCenter retiene una copia de backup antes de eliminarla. |

      Debe establecer el número de retención en 2 o superior. El valor mínimo para el número de retención es 2.

      El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.

1. En la página Replication, especifique la replicación en el sistema de almacenamiento secundario:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Actualizar SnapMirror tras crear una copia Snapshot local | Seleccione esta opción para crear copias de SnapMirror de conjuntos de backups en otro volumen (SnapMirror). |
| Actualizar SnapVault después de crear una copia Snapshot | Seleccione esta opción para realizar una replicación de backup de disco a disco. |
| Etiqueta de la política secundaria | Seleccione una etiqueta de Snapshot.<br><br>Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta.<br><br>Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria. |
| Número de reintentos con error | Introduzca el número de intentos de replicación que deben producirse antes de que se interrumpa el proceso. |

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

2. En la página Script, introduzca la ruta del script previo o script posterior que desea que el servidor SnapCenter ejecute antes o después de la operación de backup respectivamente, y el límite de tiempo que SnapCenter espera para que se ejecute el script.

   Por ejemplo, se puede ejecutar un script para actualizar capturas SNMP, automatizar alertas y enviar registros.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear grupos de recursos para sistemas de archivos Windows

Un grupo de recursos es el contenedor donde puede añadir varios sistemas de archivos que desea proteger. También deben añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar y, a continuación,

especificar la programación de backups.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **File Systems** en la lista.

   Si recientemente ha agregado un sistema de archivos a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recién añadido.

3. Haga clic en **Nuevo grupo de recursos**.
4. En la página Name del asistente, haga lo siguiente:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba el nombre del grupo de recursos.<br>El nombre del grupo de recursos no debe superar los 250 caracteres. |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Opcional: Escriba un nombre de copia de Snapshot personalizado y su formato.<br>Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |
| Etiquetar | Introduzca una etiqueta descriptiva que ayude a encontrar el grupo de recursos. |

5. En la página Resources, realice las siguientes tareas:

   a. Seleccione el host para filtrar la lista de recursos.

      Si agregó recursos recientemente, aparecerán en la lista de recursos disponibles únicamente después de actualizar la lista de recursos.

   b. En la sección Available Resources, haga clic en los sistemas de archivos de los que desea realizar backup y, a continuación, haga clic en la flecha derecha para moverlos a la sección Added.

      Si selecciona la opción **Autoselect all resources on same Storage volume**, se seleccionan todos los recursos del mismo volumen. Cuando los mueve a la sección Added, todos los recursos de ese volumen se mueven juntos.

   Para añadir un único sistema de archivos, borre la opción **Autoselect all resources on same Storage volume** y seleccione los sistemas de archivos que desea mover a la sección Added.

6. En la página Policies, ejecute las siguientes tareas:

   a. Seleccione una o varias políticas de la lista desplegable.

      Puede seleccionar cualquier directiva existente y hacer clic en **Detalles** para determinar si puede utilizar esa directiva.

      Si ninguna política cumple con sus requisitos, puede crear una nueva haciendo clic en + para iniciar el asistente de políticas.

   Las políticas seleccionadas se enumeran en la columna Policy en la sección Configure schedules for selected policies.

   a. En la sección Configure schedules for selected policies, haga clic en + En la columna Configure Schedules correspondiente a la directiva para la que desea configurar la programación.
   b. Si la política está asociada con varios tipos de programación (frecuencias), seleccione la frecuencia que desea configurar.
   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación especificando la fecha de inicio, la fecha de caducidad y la frecuencia y, a continuación, haga clic en **Finish**.

      Las programaciones configuradas aparecen en la columna Applied Schedules en la sección Configure schedules for selected policies.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter. No debe modificar las programaciones desde el programador de tareas de Windows y el agente de SQL Server.

1. En la página Notification, proporcione información de notificación de la siguiente manera:

| **Para este campo…** | **Realice lo siguiente…** |
|---|---|
| Preferencia de correo electrónico | Seleccione **Always**, **On Failure** o **On failure or warning**, para enviar correos electrónicos a destinatarios después de crear grupos de recursos de copia de seguridad, adjuntar políticas y configurar horarios. Introduzca el servidor SMTP, la línea de asunto predeterminada del correo electrónico y las direcciones de correo electrónico del remitente y destinatario. |
| De | Dirección de correo electrónico |
| Para | Dirección de correo electrónico del destinatario |
| Asunto | Línea de asunto predeterminada del correo electrónico |

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Es posible realizar un backup bajo demanda o esperar a que se produzca el backup programado.

## Realice el backup de un solo recurso bajo demanda para sistemas de archivos Windows

Si un recurso no está en un grupo de recursos, puede realizar el backup bajo demanda desde la página Resources.

### Acerca de esta tarea

Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con almacenamiento secundario, el rol asignado al usuario de almacenamiento debería incluir el privilegio «incluir toda la copia reflejada». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".

Al realizar el backup de un sistema de archivos, SnapCenter no hace backups de los LUN montados en un punto de montaje de volumen (VMP) en el sistema de archivos del que se está haciendo backup.

Si va a trabajar en un contexto de sistema de archivos de Windows, no realice backup de archivos de la base de datos. Si lo hace, se crea un backup incoherente y una posible pérdida de datos al restaurar. Para proteger los archivos de la base de datos, debe usar el plugin de SnapCenter adecuado para la base de datos (por ejemplo, plugin de SnapCenter para Microsoft SQL Server, plugin de SnapCenter para Microsoft Exchange Server o un plugin personalizado para archivos de base de datos).

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione el tipo de recurso File System y, a continuación, seleccione el recurso del que desea realizar backup.
3. Si el asistente File System - Protect no se inicia automáticamente, haga clic en **Protect** para iniciar el asistente.

   Especifique la configuración de protección, según se describe en las tareas para crear grupos de recursos.

4. Opcional: En la página Resource del asistente, introduzca un formato de nombre personalizado para la copia de Snapshot.

   Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.

5. En la página Policies, ejecute las siguientes tareas:

   a. Seleccione una o varias políticas de la lista desplegable.

      Puede seleccionar cualquier directiva existente y, a continuación, hacer clic en **Detalles** para determinar si puede utilizar esa política.

      Si ninguna política existente se ajusta a sus requisitos, puede copiar una política existente y

modificarla, o bien crear una nueva política haciendo clic en para iniciar el asistente de políticas.

Las políticas seleccionadas se enumeran en la columna Policy en la sección Configure schedules for selected policies.

a. En la sección Configure schedules for selected policies, haga clic en En la columna Configure Schedules correspondiente a la política para la cual se desea configurar la programación.

b. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación especificando la fecha de inicio, la fecha de caducidad y la frecuencia y, a continuación, haga clic en **Finish**.

   Las programaciones configuradas aparecen en la columna Applied Schedules en la sección Configure schedules for selected policies.

"Es posible que se produzca un error en las operaciones programadas"

1. En la página Notification, realice las siguientes tareas:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Preferencia de correo electrónico | Seleccione **Always**, o **On Failure**, o **On failure or warning**, para enviar correos electrónicos a destinatarios después de crear grupos de recursos de copia de seguridad, adjuntar directivas y configurar horarios.<br><br>Introduzca la información del servidor SMTP, la línea de asunto predeterminada del correo electrónico y las direcciones de correo electrónico «'a'» y «'de'». |
| De | Dirección de correo electrónico |
| Para | Dirección de correo electrónico del destinatario |
| Asunto | Línea de asunto predeterminada del correo electrónico |

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de la base de datos.

3. Haga clic en **copia de seguridad ahora**.
4. En la página Backup, realice los siguientes pasos:
   a. Si aplicó varias políticas al recurso, en la lista desplegable Policy seleccione la política que desea usar para el backup.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de

backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

b. Haga clic en **copia de seguridad**.

5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Realizar un backup de grupos de recursos para sistemas de archivos Windows

Un grupo de recursos es una agrupacion de recursos en un host o un clúster. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo. Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

**Lo que necesitará**

- Debe tener creado un grupo de recursos con una política anexada.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función asignada al usuario de almacenamiento debería incluir el privilegio «incluir toda la copia reflejada». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, la operación de backup en algunos hosts puede activarse tarde debido a problemas de red. Debe configurar el valor de MaxRetryForUninitializedHosts en web.config mediante el cmdlet Set-SmConfigSettings de PowerShell

Al realizar el backup de un sistema de archivos, SnapCenter no hace backups de los LUN montados en un punto de montaje de volumen (VMP) en el sistema de archivos del que se está haciendo backup.

Si va a trabajar en un contexto de sistema de archivos de Windows, no realice backup de archivos de la base de datos. Si lo hace, se crea un backup incoherente y una posible pérdida de datos al restaurar. Para proteger los archivos de la base de datos, debe usar el plugin de SnapCenter adecuado para la base de datos (por ejemplo, plugin de SnapCenter para Microsoft SQL Server, plugin de SnapCenter para Microsoft Exchange Server o un plugin personalizado para archivos de base de datos).

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en y seleccionando la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **Back up Now**.

Para el plugin de SnapCenter para base de datos Oracle, si tiene un grupo de recursos federados con dos bases de datos y una de ellas tiene un archivo de datos en un almacenamiento de terceros, la operación de backup se interrumpirá aunque la otra base de datos esté en un almacenamiento NetApp.

4. En la página Backup, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.
   - En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

     "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"

   - Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup. Para aumentar el tamaño del montón de Java, busque el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese script, la `do_start method` Command inicia el servicio de plugin de VMware de SnapCenter. Actualice este comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

## Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar operaciones de protección de datos.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

  No debe haber instalaciones de complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

  SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de gestión única.

- Pasos*

1. Inicie una sesión de conexión de PowerShell con mediante el cmdlet Open-SmConnection.

   En este ejemplo, se abre una sesión de PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Cree una nueva conexión con el sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

   En este ejemplo, se crea una nueva conexión con el sistema de almacenamiento:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Cree una credencial nueva mediante el cmdlet Add-SmCredential.

   En este ejemplo, se crea una nueva credencial llamada FinanceAdmin con las credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Realizar backup de recursos con cmdlets de PowerShell

Puede utilizar los cmdlets de PowerShell para realizar backup de bases de datos de SQL Server o sistemas de archivos Windows. Esto incluye la realización de backups de una base de datos de SQL Server o de un sistema de archivos de Windows incluye establecer una conexión con SnapCenter Server, determinar las instancias de la base de datos de SQL Server o los sistemas de archivos Windows, crear un grupo de recursos de backup, realizar el backup y verificar.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe añadir la conexión con el sistema de almacenamiento y crear una credencial.
- Es necesario haber añadido los hosts y detectado los recursos.
- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

Se muestra una solicitud de nombre de usuario y contraseña.

2. Cree una política de backup mediante el cmdlet Add-SmPolicy.

   En este ejemplo, se crea una nueva política de backup con el tipo de backup de SQL fullbackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

   En este ejemplo, se crea una nueva política de backup con el tipo de backup de sistema de archivos Windows CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Para detectar recursos de host se usa el cmdlet Get-SmResources.

   En este ejemplo, se determinan los recursos para el plugin de Microsoft SQL en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   En este ejemplo, se determinan los recursos para los sistemas de archivos Windows en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

   En este ejemplo, se crea un nuevo grupo de recursos de backup de base de datos de SQL con la política y los recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

En este ejemplo, se crea un nuevo grupo de recursos de backup de sistema de archivos Windows con la política y los recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Consulte el estado del trabajo de backup mediante el cmdlet Get-SmBackupReport.

   Este ejemplo muestra un informe con un resumen de todos los trabajos realizados en la fecha especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Supervisar las operaciones de backup

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

**Acerca de esta tarea**

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Monitor, haga clic en **Jobs**.

3. En la página Jobs, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
   d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
   e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

   Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

#### Supervise las operaciones en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también muestra información sobre la operación de propagación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

     Al hacer clic en una de las operaciones, se muestran sus detalles en la página Job Details.

## Cancele las operaciones de backup

Es posible cancelar las operaciones de backup que se encuentran en cola.

#### Lo que necesitará

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o el panel **Activity**.
- No es posible cancelar una operación de backup en ejecución.
- Es posible utilizar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de backup.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de**

**miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.

- Pasos*

1. Ejecute una de las siguientes acciones:

| Del… | Acción |
|---|---|
| Página Monitor | a. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**. |
| Panel de actividades | a. Tras iniciar la operación de backup, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>b. Seleccione la operación.<br>c. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

Se cancela la operación y el recurso se revierte al estado anterior.

## Consulte los backups y los clones relacionados en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario. En la página Topology, es posible ver todos los backups y clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

### Acerca de esta tarea

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
- Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.

  Los clones de un backup de un reflejo de versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejos de la vista de topología no incluye el backup de versión flexible.

-

Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

- La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.
- Si actualizó desde SnapCenter 1.1, los clones en el secundario (reflejo o almacén) no se muestran en las secciones Mirror Copies o Vault copies de la página Topology. Todos los clones creados con SnapCenter 1.1 se muestran en la sección local copies en SnapCenter 3.0.

Los clones de un backup de un reflejo de versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejos de la vista de topología no incluye el backup de versión flexible.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

   Si el recurso está protegido, se muestra la página con el resumen seleccionado.

4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el almacenamiento principal y secundario.

   La sección Summary Card muestra la cantidad total de backups y clones. Únicamente para bases de datos Oracle, la sección Summary Card también muestra el número total de backups de registro.

   Al hacer clic en el botón de actualización, se inicia una consulta del almacenamiento para ver un número preciso.

5. En la vista Administrar copias, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

   Estos detalles se muestran en forma de tabla.

6. Seleccione el backup en la tabla y haga clic en los iconos de protección de datos para realizar operaciones de restauración, clonado, cambio de nombre y eliminación.

   Los backups que figuran en el sistema de almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

   Si utiliza los plugins de personalizados de SnapCenter, no puede cambiar el nombre de los backups que están en el sistema de almacenamiento principal.

   - Si selecciona un backup de un recurso o grupo de recursos de Oracle, también puede realizar operaciones de montaje y desmontaje.
   - Si seleccionó un backup de registro de un recurso o grupo de recursos de Oracle, también puede realizar operaciones de cambio de nombre, montaje, desmontaje y eliminación.

- Si utiliza el paquete de plugins de SnapCenter para Linux y catalogó el backup con Oracle Recovery Manager (RMAN), no puede cambiar el nombre de esos backups catalogados.

7. Si desea eliminar un clon, selecciónelo en la tabla y haga clic en para eliminar el clon.

**Ejemplo que muestra copias de seguridad y clones en el almacenamiento primario**

## Quitar los backups con el cmdlet de PowerShell

Puede utilizar el cmdlet Remove-SmBackup para eliminar backups si ya no los necesita para otras operaciones de protección de datos.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Elimine uno o varios backups con el cmdlet Remove-SmBackup.

   Este ejemplo elimina dos backups según sus ID de backup:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

## Borre el número de backup secundario con cmdlets de PowerShell

Puede utilizar el cmdlet Remove-SmBackup para borrar el número de backups de backups secundarios que

no tienen copias de Snapshot. Puede ser conveniente usar este cmdlet cuando las copias de Snapshot totales que se muestran en la topología Manage Copies no coinciden con la configuración de retención de copias de Snapshot de almacenamiento secundario.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Borre el número de backups secundarios con el parámetro -CleanupSecondaryBackups.

   En este ejemplo, se borra el número de backups secundarios sin copias de Snapshot:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

# Restaurar sistemas de archivos Windows

## Restaurar backups de sistemas de archivos Windows

Puede utilizar SnapCenter para restaurar backups de sistemas de archivos. La restauración de sistema de archivos es un proceso multifase que copia todos los datos de un backup especificado en la ubicación original del sistema de archivos.

### Lo que necesitará

- Debe tener un backup del sistema de archivos.
- Si existe una operación programada, como una operación de backup, en curso para un sistema de archivos, debe cancelarse esa operación antes de poder iniciar una operación de restauración.
- Solo puede restaurar un backup de sistema de archivos a la ubicación original, no a una ruta alternativa.

  No puede restaurar un solo archivo desde un backup porque el sistema de archivos restaurado sobrescribe los datos en la ubicación original del sistema de archivos. Para restaurar un solo archivo desde un backup del sistema de archivos, debe clonar el backup y acceder al archivo en el clon.

- No puede restaurar un sistema o volumen de arranque.

- SnapCenter puede restaurar los sistemas de archivos de un clúster de Windows sin que el grupo de clústeres esté sin conexión.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Para filtrar la lista de recursos, seleccione las opciones File System y Resource Group.
  3. Seleccione un grupo de recursos de la lista y, a continuación, haga clic en **Restaurar**.
  4. En la página backups, seleccione si desea restaurar desde los sistemas de almacenamiento principal o secundario y luego seleccione un backup para restaurar.
  5. Seleccione sus opciones en el asistente Restore.
  6. Puede introducir la ruta y los argumentos del script previo o script posterior que desea que SnapCenter ejecute antes o después de la operación de restauración, respectivamente.

     Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

  7. En la página Notification, seleccione una de las siguientes opciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Registre los eventos del servidor SnapCenter en el syslog del sistema de almacenamiento | Seleccione esta opción para registrar los eventos de servidor de SnapCenter en el syslog del sistema de almacenamiento. |
| Envíe una notificación de AutoSupport sobre las operaciones con errores al sistema de almacenamiento | Seleccione esta opción para enviar información sobre las operaciones con errores a NetApp mediante AutoSupport. |
| Preferencia de correo electrónico | Seleccione **Always**, **On Failure** o **On failure or warning** para enviar mensajes de correo electrónico a los destinatarios después de restaurar las copias de seguridad. Introduzca el servidor SMTP, la línea de asunto predeterminada del correo electrónico y las direcciones de correo electrónico del remitente y destinatario. |

  8. Revise el resumen y, a continuación, haga clic en **Finalizar**.
  9. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Si el sistema de archivos restaurado contiene una base de datos, debe también restaurar la base de datos. Si no restaura la base de datos, la base de datos puede quedar en estado no válido. Para obtener información sobre cómo restaurar bases de datos, consulte la guía de protección de datos de esa base de datos.

## Restaurar recursos mediante los cmdlets de PowerShell

La restauración de un backup de recursos incluye el inicio de una sesión de conexión con el servidor SnapCenter, el listado de los backups y la recuperación de información de los backups, y la restauración de un

backup.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Para recuperar la información sobre los backups que desea restaurar, puede usar los cmdlets Get-SmBackup y Get-SmBackupReport.

   Este ejemplo muestra información sobre todos los backups disponibles:

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

   En este ejemplo, se muestra información detallada sobre el backup del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

1. Puede restaurar los datos del backup mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Supervisar operaciones de restauración

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

### Acerca de esta tarea

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso

- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

## Cancele las operaciones de restauración

Es posible cancelar los trabajos de restauración que se encuentran en cola.

Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.

**Acerca de esta tarea**

- Es posible cancelar una operación de restauración en cola desde la página Monitor o el panel Activity.
- No se puede cancelar una operación de restauración en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está desactivado para operaciones de restauración que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de

restauración en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione el trabajo y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar la operación de restauración, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

# Clonar sistemas de archivos Windows

## Clonar desde un backup de sistema de archivos Windows

Puede utilizar SnapCenter para clonar un backup de sistema de archivos Windows. Si desea copiar un archivo que se eliminó o modificó por error, puede clonar un backup y acceder a dicho archivo en el clon.

**Lo que necesitará**

- Debe haberse preparado para la protección de datos completando ciertas tareas, como añadir hosts, identificar recursos y crear conexiones de máquina virtual de almacenamiento (SVM).
- Debe tener un backup del sistema de archivos.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- No puede clonar un grupo de recursos. Solo puede clonar backups individuales de sistema de archivos.
- Si un backup reside en una máquina virtual con un disco VMDK, SnapCenter no puede clonar el backup en un servidor físico.
- Si clona un clúster de Windows (por ejemplo, un LUN compartido o un LUN con volumen compartido de clúster (CSV), el clon se almacena como LUN dedicado en el host que especifique.
- Para una operación de clonado, el directorio raíz del punto de montaje de volumen no puede ser un directorio compartido.
- No puede crear un clon en un nodo que no sea el nodo de inicio para el agregado.
- No puede programar operaciones de clon recurrentes (ciclo de vida de clon) para sistemas de archivos Windows. Solo puede clonar un backup bajo demanda.
- Si se mueve un LUN que contiene un clon de un volumen nuevo, SnapCenter ya no puede admitir el clon.

Por ejemplo, no se puede usar SnapCenter para eliminar ese clon.

- No es posible clonar entre entornos. Por ejemplo, la clonación de un disco físico a un disco virtual o viceversa.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **File Systems** en la lista.
  3. Seleccione el host.

     La vista de topología se muestra automáticamente si el recurso está protegido.
  4. Desde la lista de recursos, seleccione el backup que desea clonar y luego haga clic en el icono de clonar.
  5. En la página Options, haga lo siguiente:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Clone el servidor | Elija el host donde se debe crear el clon. |
| «"punto de montaje auto assign» o «"asignar automáticamente punto de montaje de volumen en ruta"». | Elija si asignar automáticamente un punto de montaje o un punto de montaje de volumen en una ruta.<br><br>Auto assign volume Mount point under path: El punto de montaje en una ruta permite proporcionar un directorio específico donde se crearán los puntos de montaje. Antes de elegir esta opción debe comprobar que el directorio esté vacío. Si hay un backup en el directorio, el backup estará en estado no válido tras la operación de montaje. |
| Ubicación del archivo | Elija una ubicación de archivado si va a clonar un backup secundario. |

  6. En la página Script, especifique los scripts previos y posteriores que desea ejecutar.
  7. Revise el resumen y, a continuación, haga clic en **Finalizar**.
  8. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Clonar backups mediante cmdlets de PowerShell

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

- Pasos*
  1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Enumere los backups que pueden clonarse mediante el cmdlet Get-SmBackup o Get-SmResourceGroup.

   Este ejemplo muestra información sobre todos los backups disponibles:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                         11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                         11:23:17 AM
```

   En este ejemplo, se muestra información sobre un grupo de recursos especificado, sus recursos y sus políticas asociadas:

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
```

```
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
```

```
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Inicie una operación de clonado a partir de un backup existente con el cmdlet New-SmClone.

   En este ejemplo, se crea un clon a partir de un determinado backup con todos los registros:

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

   En este ejemplo, se crea un clon en una instancia concreta de Microsoft SQL Server:

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Puede consultar el estado del trabajo de clonado mediante el cmdlet Get-SmCloneReport.

   En este ejemplo, se muestra un informe de clonado con el correspondiente ID de trabajo:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Supervise las operaciones de clonación

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

-

En curso

- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Clonar**.
   d. En la lista desplegable **Estado**, seleccione el estado del clon.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Cancele las operaciones de clonado

Es posible cancelar las operaciones de clonado que se encuentran en cola.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de clonado.

**Acerca de esta tarea**

- Es posible cancelar una operación de clonado en cola desde la página Monitor o el panel Activity.
- No se puede cancelar una operación de clonado en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de clonado en cola.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de clonación en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione la operación y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar la operación de clonado, haga clic en  En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

## Divida un clon

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

### Acerca de esta tarea

- No se puede ejecutar la operación de división de clones en un clon intermedio.

  Por ejemplo, después de crear el clon 1 a partir de un backup de la base de datos, puede realizar un backup del clon 1 y luego clonar este backup (que sería el clon 2). Una vez creado el clon 2, el clon 1 se convierte en un clon intermedio y la operación de división de clones puede hacerse con el clon 1. No obstante, esta operación también puede ejecutarse con el clon 2.

  Después de dividir el clon 2, puede ejecutar la operación de división de clones con el clon 1, ya que este deja de ser el clon intermedio.

- Cuando divide un clon, se eliminan las copias de backup y los trabajos de clonado del clon.
- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Asegúrese de que el volumen o el agregado del sistema de almacenamiento estén en línea.
- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página **Recursos**, seleccione la opción adecuada en la lista Ver:

     | Opción | Descripción |
     | --- | --- |
     | Para aplicaciones de base de datos | Seleccione **base de datos** en la lista View. |
     | Para sistemas de archivos | Seleccione **Ruta** en la lista Ver. |

  3. Seleccione el recurso adecuado de la lista.

Se muestra la página con el resumen.

4. En la vista Manage Copies, seleccione el recurso clonado (por ejemplo, la base de datos o el LUN) y, a continuación, haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
6. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

   La operación de división de clones se detiene si se reinicia el servicio de SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clones y luego volver a intentar la operación de división de clones.

   Si necesita más o menos tiempo de sondeo para comprobar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer un intervalo para que SMCore sondee el estado de la operación de división de clones. El valor se registra en milisegundos; el predeterminado son 5 minutos.

   Por ejemplo:

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

+
Se produce un error en la operación de inicio de división de clones si hay un backup, una restauración u otra división de clones en curso. Solo debe reiniciar la operación de división de clones una vez que hayan finalizado las operaciones en ejecución.

**Más información**

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

# Proteger las bases de datos de Microsoft Exchange Server

## Conceptos del plugin de SnapCenter para Microsoft Exchange Server

### Información general sobre el plugin de SnapCenter para Microsoft Exchange Server

El plugin de SnapCenter para Microsoft Exchange Server es un componente en el lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de bases de datos de Exchange. El plugin para Exchange automatiza el backup y la restauración de bases de datos de Exchange en el entorno de SnapCenter.

Cuando se instala el plugin para Exchange, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear copias de reflejo de conjuntos de backups en otro volumen, y también con la tecnología SnapVault de NetApp para realizar replicaciones de backup disco a disco para cumplimiento de normativas o fines de archivado.

Si desea restaurar y recuperar correos electrónicos o buzones en lugar de completar base de datos de Exchange, puede utilizar el software Single Mailbox Recovery (SMBR).
NetApp® Single Mailbox Recovery ha llegado al final de la disponibilidad (EOA) el 12 de mayo de 2023. NetApp continuará prestando soporte a los clientes que hayan adquirido capacidad, mantenimiento y soporte de sus buzones mediante números de referencia de marketing introducidos el 24 de junio de 2020, durante el periodo de concesión de soporte.

Single Mailbox Recovery de NetApp es un producto de partner que proporciona Ontrack. Ontrack PowerControls ofrece capacidades similares a las de Single Mailbox Recovery de NetApp. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls desde Ontrack (hasta licensingteam@ontrack.com) para la recuperación granular de buzones.

### Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft Exchange Server

Es posible usar el plugin para Exchange a fin de realizar backup y restaurar bases de datos de Exchange Server.

- Ver y gestionar un inventario activo de DAG, bases de datos y conjuntos de réplicas de Exchange
- Definir políticas que ofrezcan opciones de protección para automatización de backup
- Asigne políticas a grupos de recursos
- Proteger grupos de disponibilidad de base de datos y bases de datos individuales
- Realizar backup de bases de datos de buzón de Exchange primarias y secundarias
- Restaurar bases de datos de backups primarios y secundarios

## Tipos de almacenamiento compatibles con el plugin de SnapCenter para Microsoft Windows y Microsoft Exchange Server

SnapCenter es compatible con una gran variedad de tipos de almacenamiento, tanto en máquinas físicas como virtuales. Antes de instalar el paquete para el host, es necesario verificar que el tipo de almacenamiento sea compatible.

Windows Server es compatible con el aprovisionamiento y la protección de datos de SnapCenter. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
|---|---|---|---|
| Servidor físico | LUN conectados a FC | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Servidor físico | LUN conectados a iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | |
| Máquina virtual de VMware | LUN de RDM conectados por un adaptador de bus de host FC o iSCSI | Cmdlets de PowerShell | Solo compatibilidad física<br>Los VMDK no son compatibles. |
| Máquina virtual de VMware | LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Los VMDK no son compatibles. |

| Máquina | Tipo de almacenamiento | Aprovisionamiento con | Notas de soporte |
| --- | --- | --- | --- |
| Máquina virtual Hyper-V. | LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | Para aprovisionar LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual se debe usar Hyper-V Manager.<br>No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |
| Máquina virtual Hyper-V. | LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI | Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell | No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp. |

## Privilegios mínimos requeridos de ONTAP

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| event generate-autosupport-log |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| se muestra el historial del trabajo<br>detención de trabajo |
| lun<br>lun create<br>eliminación de lun<br>igroup de lun añadido<br>crear lun igroup<br>lun igroup eliminado<br>cambio de nombre de lun igroup<br>lun igroup show<br>asignación de lun de nodos adicionales<br>se crea la asignación de lun<br>se elimina la asignación de lun<br>asignación de lun quitar nodos de generación de informes<br>se muestra el mapa de lun<br>modificación de lun<br>movimiento de lun en volumen<br>lun desconectada<br>lun conectada<br>reserva persistente de lun clara<br>cambio de tamaño de lun<br>serie de lun<br>muestra de lun |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| regla adicional de la política de snapmirror<br>regla de modificación de la política de snapmirror<br>regla de eliminación de la política de snapmirror<br>la política de snapmirror<br>restauración de snapmirror<br>de snapmirror<br>historial de snapmirror<br>actualización de snapmirror<br>conjunto de actualizaciones de snapmirror<br>destinos de listas de snapmirror |
| versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| crear el clon de volumen |
| show de clon de volumen |
| inicio de división de clon de volumen |
| detención de división de clon de volumen |
| cree el volumen |
| destrucción del volumen |
| crear el archivo de volumen |
| uso show-disk del archivo de volumen |
| volumen sin conexión |
| volumen en línea |
| modificación del volumen |
| crear el qtree de volúmenes |
| eliminación de qtree de volumen |
| modificación del qtree del volumen |
| se muestra volume qtree |
| restricción de volumen |
| visualización de volumen |
| crear snapshots de volumen |
| eliminación de snapshots de volumen |
| modificación de las copias de snapshot de volumen |
| cambio de nombre de copias de snapshot de volumen |
| restauración de copias snapshot de volumen |
| archivo de restauración de snapshots de volumen |
| visualización de copias de snapshot de volumen |
| desmonte el volumen |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| vserver cifs |
| vserver cifs share create |
| eliminación de vserver cifs share |
| se muestra vserver shadowcopy |
| visualización de vserver cifs share |
| visualización de vserver cifs |
| política de exportación de vserver |
| creación de política de exportación de vserver |
| eliminación de la política de exportación de vserver |
| creación de reglas de política de exportación de vserver |
| aparece la regla de política de exportación de vserver |
| visualización de la política de exportación de vserver |
| vserver iscsi |
| se muestra la conexión iscsi del vserver |
| se muestra vserver |

| Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| interfaz de red |
| se muestra la interfaz de red |
| vserver |

## Preparar los sistemas de almacenamiento para la replicación con SnapMirror y SnapVault

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en

el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

> SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

## Defina una estrategia de backup para recursos de servidor de Exchange

Definir una estrategia de backup antes de crear las tareas de backup ayuda a garantizar que se cuente con todos los backups necesarios para restaurar correctamente las bases de datos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el objetivo de punto de recuperación contribuyen a la estrategia de backup.

### Tipos de backups compatibles con la base de datos de Exchange

Los backups de buzones de correo de Exchange que usan SnapCenter requieren elegir el tipo de recurso, como bases de datos y DAG. Se aprovecha la tecnología de copia de Snapshot para crear copias en línea y de solo lectura de los volúmenes donde residen los recursos.

| Tipo de backup | Descripción |
|---|---|
| Backup completo y de registros | Realiza un backup de las bases de datos y de todos los registros de transacciones, incluidos los registros acortados.<br><br>Una vez completado un backup completo, Exchange Server acorta los registros de transacciones que ya están confirmados en la base de datos.<br><br>En términos generales, debe elegir esta opción. Sin embargo, si el tiempo de backup es corto, puede optar por no ejecutar un backup del registro de transacciones junto con el backup completo. |
| Backup completo | Realiza un backup de las bases de datos y los registros de transacciones.<br><br>No se realiza un backup de los registros de transacciones acortados. |

| Tipo de backup | Descripción |
| --- | --- |
| Backup de registros | Realiza un backup de todos los registros de transacciones.<br><br>Los registros acortados que ya están confirmados en la base de datos no se respaldan. Si programa backups del registro de transacciones frecuentes entre backups completos de la base de datos, puede elegir puntos de recuperación granulares. |

**Programaciones de backups para plugins de bases de datos**

La frecuencia de los backups (tipo de programación) se especifica en las políticas; la programación de los backups se especifica en la configuración del grupo de recursos. El factor más crítico para determinar la frecuencia o la programación de los backups es la tasa de cambio del recurso y la importancia de los datos. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores son la importancia del recurso para la organización, el SLA y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso en el caso de un recurso utilizado intensivamente, no existe el requisito de ejecutar un backup completo más de una o dos veces al día. Por ejemplo, es posible que sea suficiente realizar backups regulares de registros de transacciones para garantizar los backups necesarios Cuanto mayor sea la frecuencia con que realiza backups de las bases de datos, menos registros de transacciones deberá utilizar SnapCenter en el momento de la restauración, lo que puede dar como resultado operaciones más rápidas.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de los backups (cada cuánto tiempo deben realizarse los backups), denominada *schedule type* para algunos plugins, forma parte de la configuración de una política. Se puede seleccionar una frecuencia de backups por hora, por día, por semana o por mes para la política. Si no selecciona ninguna de estas frecuencias, la política creada es de sólo bajo demanda. Puede acceder a las directivas haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

  Las programaciones de los backups (el momento exacto en que se realizan los backups) forman parte de una configuración de grupo de recursos. Por ejemplo, si tiene un grupo de recursos que posee una política configurada para backups semanales, quizás sea conveniente configurar la programación para que realice backups todos los jueves a las 00:10. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **grupos de recursos**.

**Cantidad de tareas de backup necesarias para bases de datos**

Algunos factores que determinan la cantidad de trabajos de backup que se necesitan son el tamaño del recurso, la cantidad de volúmenes que se usan, la tasa de cambio del recurso y el acuerdo de nivel de

servicio.

### Convenciones de nomenclatura de backups

Es posible usar la convención de nomenclatura de copia Snapshot predeterminada o usar una convención de nomenclatura personalizada. La convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de las copias de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La copia Snapshot usa la siguiente convención de nomenclatura predeterminada:

```
resourcegroupname_hostname_timestamp
```

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre de host.
- *03-12-2015_23.17.26* es la fecha y la marca de hora.

Como alternativa, puede especificar el formato de nombre de la copia Snapshot mientras protege los recursos o grupos de recursos seleccionando **usar formato de nombre personalizado para copia Snapshot**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la copia de Snapshot.

### Opciones de retención de backups

Es posible elegir la cantidad de días durante los cuales se retendrán las copias de backup o especificar la cantidad de copias de backup que se desean retener, con un máximo de 255 copias en ONTAP. Por ejemplo, una organización puede necesitar retener 10 días de copias de backup o 130 copias de backup.

Al crear una política, es posible especificar las opciones de retención para cada tipo y programación de backup.

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

SnapCenter elimina los backups previos que tengan etiquetas de retención que coincidan con el tipo de programación. Si se modifica el tipo de programación para el recurso o el grupo de recursos, los backups con la etiqueta del tipo de programación anterior podrían conservarse en el sistema.

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

### Cuánto tiempo se retienen los backups de registros de transacciones en el volumen de almacenamiento de origen para Exchange Server

El plugin de SnapCenter para Microsoft Exchange Server necesita backups de registros de transacciones para ejecutar operaciones de restauración de último minuto, que restauran la base de datos a un momento entre dos backups completos.

Por ejemplo, si el plugin para Exchange hizo un backup completo de los registros de transacciones más a las 8:00 y otro backup completo de los registros de transacciones a las 8:00 p. m., se puede usar el último backup de registros de transacciones para restaurar la base de datos a cualquier momento entre las 5:00 y las 5:00 Si no se cuenta con registros de transacciones, el plugin para Exchange solamente puede ejecutar operaciones de restauración a un momento específico, que restaura una base de datos en el momento en que el plugin para Exchange finalizó un backup completo.

En general, se requieren operaciones de restauración de último minuto únicamente durante un día o dos. De forma predeterminada, SnapCenter conserva un mínimo de dos días.

## Definir una estrategia de restauración para bases de datos de Exchange

Definir una estrategia de restauración para servidor de Exchange permite restaurar correctamente la base de datos.

### Orígenes para una operación de restauración en Exchange Server

Es posible restaurar una base de datos de Exchange Server desde una copia de backup en el almacenamiento primario.

Es posible restaurar bases de datos solo desde el almacenamiento primario.

### Tipos de operaciones de restauración compatibles con Exchange Server

Es posible usar SnapCenter para ejecutar diferentes tipos de operaciones de restauración de los recursos de Exchange.

- Restauración de último minuto
- Restauración a un momento específico

#### Restauración de último minuto

En una operación de restauración de último minuto, se recuperan las bases de datos hasta el punto de error. SnapCenter usa la siguiente secuencia para este proceso:

1. Restaura las bases de datos desde el backup completo de la base de datos que se seleccione.
2. Aplica todos los registros de transacciones incluidos en el backup, así como los nuevos registros que se hayan creado desde el backup más reciente.

   Se mueven los registros de transacciones y se aplican a las bases de datos seleccionadas.

   Exchange crea una nueva cadena de registro una vez que finaliza la restauración.

   **Mejor práctica:** se recomienda realizar una nueva copia de seguridad completa y de registro una vez finalizada la restauración.

   Una operación de restauración de último minuto requiere un conjunto de registros de transacciones contiguos.

   Una vez finalizada una restauración de último minuto, el backup usado para la restauración solo está disponible para las operaciones de restauración a un momento específico.

   Si no se necesita la funcionalidad de restauración de último minuto para todos los backups, es posible

configurar la retención de backup de los registros de transacciones del sistema mediante las políticas de backup.

#### Restauración a un momento específico

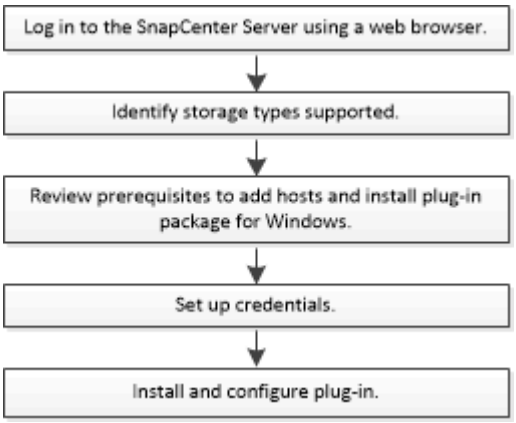
En una operación de restauración a un momento específico, las bases de datos se restauran únicamente a un punto específico. Esta operación se ejecuta en las siguientes situaciones:

- La base de datos se restaura a un punto específico en un registro de transacciones incluido en un backup.
- Se restaura la base de datos, y solo se aplica un subconjunto de los registros de transacciones del backup.

# Instale el plugin de SnapCenter para Microsoft Exchange Server

## Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Exchange Server

Debe instalar y configurar el plugin de SnapCenter para Microsoft Exchange Server si desea proteger las bases de datos de Exchange.




## Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft Exchange Server

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Debe usar Microsoft Exchange Server 2013, 2016 o 2019 para configuraciones independientes y de grupos de disponibilidad de base de datos.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Si gestiona nodos de clúster en SnapCenter, debe tener un usuario con privilegios de administrador para todos los nodos del clúster.

- Debe tener un usuario con permisos de administrador en Exchange Server.
- Si SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya se han instalado, debe anular el registro del proveedor de hardware VSS usado por SnapDrive para Windows antes de que instale el plugin para Exchange en el mismo Exchange Server para garantizar una protección de datos exitosa usando SnapCenter.
- Si SnapManager para Microsoft Exchange Server y el plugin para Exchange están instalados en el mismo servidor, debe suspender o eliminar todas las programaciones del programador de Windows creadas por SnapManager para Microsoft Exchange Server.
- El host debe poder resolverse con el nombre de dominio completo (FQDN) del servidor. Si el archivo hosts se modifica para que pueda resolverse y si se especifican tanto el nombre corto como el FQDN en el archivo hosts, cree una entrada en el archivo hosts SnapCenter con el siguiente formato: *<ip_address> <host_fqdn> <host_name>*.
- Compruebe que los puertos siguientes no estén bloqueados en el firewall; de lo contrario, la operación de añadir host fallará. Para resolver este problema, debe configurar el intervalo de puertos dinámico. Para obtener más información, consulte "Documentación de Microsoft".
  - Intervalo de puertos 50000 - 51000 para Windows 2016 y Exchange 2016
  - Intervalo de puertos 6000 - 6500 para Windows 2012 R2 y Exchange 2013
  - Intervalo de puertos 49152 - 65536 para Windows 2019

Para identificar el intervalo de puertos, ejecute los siguientes comandos:

- netsh int ipv4 muestran dynamicport tcp
- netsh int ipv4 muestran dynamicport udp
- netsh int ipv6 muestra dynamicport tcp
- netsh int ipv6 muestra dynamicport udp

### Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows

Antes de instalar el paquete de plugins de SnapCenter para Windows, debe estar familiarizado con algunos requisitos básicos de espacio y tamaño del sistema host.

| Elemento | Requisitos |
|---|---|
| Sistemas operativos | Microsoft Windows<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |

| Elemento | Requisitos |
| --- | --- |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 5 GB<br><br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |
| Paquetes de software obligatorios | • Microsoft .NET Framework 4.5.2 o posterior<br>• Windows Management Framework (WMF) 4.0 o posterior<br>• PowerShell 4.0 o posterior<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |

**Privilegios de servidor de Exchange necesarios**

Para habilitar SnapCenter y añadir un servidor de Exchange o DAG, y para instalar el plugin de SnapCenter para Microsoft Exchange Server en un host o DAG, es necesario configurar SnapCenter con las credenciales para un usuario con un conjunto mínimo de privilegios y permisos.

Se necesita un usuario de dominio con privilegios de administrador local y con permisos de inicio de sesión local en el host de Exchange remoto, además de permisos administrativos en todos los nodos del DAG. El usuario de dominio debe contar con los siguientes permisos mínimos:

- Add-MailboxDatabaseCopy
- Desmontar base de datos
- Get-AdServerSettings
- Get-DatabaseDisponabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase

- Move-DatabasePath -ConfigurationOnly:$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

### Configurar GMSA en Windows Server 2012 o posterior

Antes de instalar el paquete de plugins de SnapCenter para Windows, debe estar familiarizado con algunos requisitos básicos de espacio y tamaño del sistema host.

| Elemento | Requisitos |
| --- | --- |
| Sistemas operativos | Microsoft Windows<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 5 GB<br><br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |

| Elemento | Requisitos |
| --- | --- |
| Paquetes de software obligatorios | • Microsoft .NET Framework 4.5.2 o posterior<br>• Windows Management Framework (WMF) 4.0 o posterior<br>• PowerShell 4.0 o posterior<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |

## Configure credenciales para el plugin de SnapCenter para Windows

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar el paquete de plugins y credenciales adicionales para realizar operaciones de protección de datos en bases de datos.

**Acerca de esta tarea**

Debe configurar credenciales para instalar plugins en hosts de Windows. Aunque puede crear credenciales para Windows después de implementar hosts e instalar plugins, lo mejor es crear credenciales después de añadir SVM antes de implementar hosts e instalar plugins.

Configure las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.

Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al nombre de usuario.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Settings, haga clic en **Credential**.
  3. Haga clic en **Nuevo**.

     Se mostrará la ventana Credential.

  4. En la página Credential, haga lo siguiente:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de credencial | Escriba un nombre para la credencial. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario | Introduzca el nombre de usuario utilizado para autenticación.<br>• Administrador de dominio o cualquier miembro del grupo de administradores<br>Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>• Administrador local (sólo para grupos de trabajo)<br>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: `UserName` |
| Contraseña | Introduzca la contraseña usada para autenticación. |
| Autenticación | Seleccione Windows como el modo de autenticación. |

5. Haga clic en **Aceptar**.

## Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

**Lo que necesitará**

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. Reinicie el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

1. Asigne los privilegios administrativos al GMSA configurado en el host.
2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

   El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

## Añada hosts e instale el plugin para Exchange

Puede utilizar la página SnapCenter **Agregar host** para agregar hosts de Windows. El plugin para Exchange se instala automáticamente en el host especificado. Este es el método recomendado para la instalación de plugins. Puede añadir un host e instalar un plugin para un host individual o para un clúster.

**Lo que necesitará**

- Debe ser un usuario al que se ha asignado una función que tiene permisos para instalar y desinstalar plugins, como el administrador de SnapCenter
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- El servicio de cola de mensajes debe estar en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos. Para obtener más información, consulte"Configurar la cuenta de servicio administrado de grupo en Windows Server 2012 o posterior".

**Acerca de esta tarea**

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

Puede añadir un host e instalar paquetes de plugins para un host individual o para un clúster. Si instala plugins en un clúster (Exchange DAG), se instalarán en todos los nodos del clúster aunque algunos nodos no tengan base de datos en las LUN de NetApp.

El plugin para Exchange depende del paquete de plugins de SnapCenter para Windows, y las versiones deben ser las mismas. Durante la instalación del plugin para Exchange, el paquete de plugins de SnapCenter para Windows está seleccionado de forma predeterminada y se instala junto con el proveedor de hardware VSS.

Si SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya están instalados, Además, desea instalar el plugin para Exchange en el mismo servidor de Exchange, debe anular el registro del proveedor de hardware VSS que utiliza SnapDrive para Windows porque es incompatible con el proveedor de hardware de VSS instalado con el plugin para Exchange y el paquete de plugins de SnapCenter para Windows.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.

2. Compruebe que **Managed hosts** está seleccionado en la parte superior.
3. Haga clic en **Agregar**.
4. En la página **hosts**, haga lo siguiente:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de host | Seleccione **Windows** como tipo de host.<br><br>El servidor de SnapCenter añade el host y, después, instala en el host el plugin para Windows y el plugin para Exchange, si no están ya instalados.<br><br>El plugin para Windows y el plugin para Exchange deben tener la misma versión. Si se instaló anteriormente otra versión del plugin para Windows, SnapCenter actualiza la versión como parte de la instalación. |
| Nombre de host | Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.<br><br>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el nombre de dominio completamente cualificado (FQDN).<br><br>Una dirección IP es compatible para los hosts de dominio que no son de confianza solo si se resuelve en el FQDN.<br><br>Puede introducir las direcciones IP o el FQDN de uno de los siguientes:<br><br>• Host independiente<br>• DAG de Exchange<br><br>Si va a añadir un host mediante SnapCenter y forma parte de un subdominio, debe proporcionar el FQDN.<br><br>También puede añadir el clúster DAG sin IP mediante la dirección IP o el FQDN de uno de los nodos del clúster DAG. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Credenciales | Seleccione el nombre de la credencial que ha creado o cree las credenciales nuevas.<br><br>Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte los detalles de cómo crear una credencial.<br><br>Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado.<br><br>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. |

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.

   Si selecciona Plug-in for Exchange, el plugin de SnapCenter para Microsoft SQL Server se desactiva automáticamente. Microsoft recomienda no instalar en el mismo sistema el servidor SQL y el de Exchange debido al volumen de memoria necesario y al uso de otros recursos que requiere Exchange.

6. (Opcional) haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto.<br><br>El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. |
| Ruta de instalación | La ruta predeterminada es `C:\Program Files\NetApp\SnapCenter`.<br><br>Opcionalmente, puede personalizar la ruta. |
| Añada todos los hosts del DAG | Seleccione esta casilla de comprobación cuando añada un DAG. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Omitir comprobaciones previas a la instalación | Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin. |
| Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in | Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de complemento.<br><br>Proporcione el nombre de GMSA con el siguiente formato: *Domainname\accountName$*.<br><br>GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows. |

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para determinar si cumple los requisitos de instalación del plugin. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia que correspondan.

   Si el error está relacionado con el espacio en disco o la RAM, puede actualizar el archivo web.config ubicado en `C:\Program Files\NetApp\SnapCenter` Webapp para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero debe solucionar el problema.

   En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

1. Supervise el progreso de la instalación.

## Instale el plugin para Exchange desde el host del servidor de SnapCenter mediante cmdlets de PowerShell

Tiene que instalar el plugin para Exchange desde la interfaz gráfica de usuario de SnapCenter. Si no quiere utilizar la interfaz gráfica de usuario, puede utilizar los cmdlets de PowerShell en el host del servidor de SnapCenter o en un host remoto.

### Lo que necesitará

- El servidor SnapCenter debe estar instalado y configurado.
- Tiene que ser el administrador local en el host o un usuario con privilegios administrativos.
- Tiene que ser un usuario con un rol asignado que tenga el plugin, así como permisos de instalación y desinstalación, como el administrador de SnapCenter
- Tiene que haber revisado los requisitos de instalación y los tipos de configuraciones compatibles antes de

instalar el plugin para Exchange.

- El host en el que desee instalar el plugin para Exchange tiene que ser un host de Windows.
- Pasos*

1. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet _Open-SmConnection y, a continuación, introduzca sus credenciales.
2. Añada el host en el que desee instalar el plugin para Exchange con el cmdlet *Add-SmHost* con los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

El host puede ser independiente o un DAG. Si especifica un DAG, el parámetro *-IsDAG* es obligatorio.

1. Instale el plugin para Exchange mediante el cmdlet *Install-SmHostPackage* con los parámetros necesarios.

   Este comando instala el plugin para Exchange en el host especificado y, a continuación, registra el plugin con SnapCenter.

## Instale el plugin de SnapCenter para Exchange silenciosamente desde la línea de comandos

Debe instalar el plugin para Exchange desde la interfaz de usuario de SnapCenter. Sin embargo, si no puede hacerlo por algún motivo, puede ejecutar el programa de instalación del plugin para Exchange sin supervisión en el modo silencioso desde la línea de comandos de Windows.

**Lo que necesitará**

- Debe tener un backup de los recursos de Microsoft Exchange Server.
- Debe haber instalado los paquetes de plugins de SnapCenter.
- Debe eliminar la versión anterior del plugin de SnapCenter para Microsoft SQL Server antes de instalar.

  Para obtener más información, consulte "Cómo instalar un plugin de SnapCenter de forma manual y directa desde el host del plugin".

- Pasos*

1. Compruebe si existe una carpeta *C:\temp* en el host del plugin y que el usuario que ha iniciado sesión tiene acceso completo a ella.
2. Descargue el plugin de SnapCenter para Microsoft Windows desde *C:\ProgramData\NetApp\SnapCenter\Package* Repository.

   Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

3. Copie el archivo de instalación en el host en el que desea instalar el plugin.
4. Desde el símbolo del sistema de Windows en el host local, desplácese hasta el directorio en el que guardó los archivos de instalación del plugin.

5. Introduzca el siguiente comando para instalar y sustituya las variables con sus datos:

   *Snapcenter_Windows_host_plugin.exe"/silent /DEBUGLOG"<Debug_Log_Path>" /log"<Log_Path>" BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Install_Directory_Path>" BI_SERVICEACCOUNT=<domain\administrator> BI_SERVICEPWD=<password> FeatureInstall=HPPW,SCW,SCE*

   Por ejemplo:

   _C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_Windows_host_plugin.exe"/silent /Featurelog"C:\HPPW_SCSQL_Install.log" /log"C:\TEMP" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"_DEBUGENG=SERVIPW_Administrator=contraseña_COVISPW_SEW_SEW_Administrator=SERVISPW_SEW_SEW_DURBW_SEW_SEAT=Install_SEAT=Administrador_SEBURB

   > Todos los parámetros que se pasan durante la instalación del plugin para Exchange distinguen entre mayúsculas y minúsculas.

   a. */silent /DEBUGLOG"C:\InstallDEBUNT.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Archivos de programa" BI_SERVICCOUNT=demo\Administrator BI_SERVICEPWD=Netapp1! ISFeatureInstall=HPPW,SCW*

      Introduzca los siguientes valores para las variables:

| Variable | Valor |
|---|---|
| */DEBUGLOG"<Debug_Log_Path>* | Indique el nombre y la ubicación del archivo de registro del instalador de la suite, como en el ejemplo siguiente:<br><br>*Setup.exe /DEBUGLOG"C:\PathToLog\setupexe.log* |
| BI_SNAPCENTER_PORT | Indique el puerto en el que SnapCenter se comunica con SMCore. |
| SUITE_INSTALLDIR | Indique el directorio de instalación para el paquete de plugins del host. |
| BI_SERVICEACCOUNT | Indique la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows. |
| BI_SERVICEPWD | Indique la contraseña para la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows. |
| ISFeatureInstall | Indique la solución que debe aplicar SnapCenter en un host remoto. |

1. Supervise el programador de tareas de Windows, el archivo de registro de instalación principal *C:\Installdebug.log* y los archivos de instalación adicionales en *C:\Temp*.

2. Supervise el directorio *%temp%* para comprobar si los instaladores *msiexe.exe* están instalando el software sin errores.

> La instalación del plugin para Exchange registra el plugin en el host y no en el servidor de SnapCenter. Es posible registrar el plugin en SnapCenter Server. Para ello, se debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Una vez añadido el host, el plugin se detecta automáticamente.

## Supervise el estado de instalación del paquete de plugins de SnapCenter

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de instalación.
     e. Haga clic en **aplicar**.
  4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configurar certificado de CA

### Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

### Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

- Pasos*

1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
2. En la ventana **Agregar o quitar complementos**, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
3. En la ventana del complemento **certificados**, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
|---|---|
| Importar clave privada | Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**. |
| Importar formato de archivo | No realice cambios; haga clic en **Siguiente**. |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |
| Finalización del Asistente para importación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación. |

El certificado de importación debe incluirse con la clave privada (los formatos admitidos son: *.pfx, *.p12, *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

### Obtenga la huella digital del certificado de CA

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

- Pasos*
  1. Realice lo siguiente en la interfaz gráfica de usuario:
     a. Haga doble clic en el certificado.
     b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
     c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
     d. Copie los caracteres hexadecimales del cuadro.
     e. Quite los espacios entre los números hexadecimales.

        Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

  2. Realice lo siguiente desde PowerShell:
     a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

        *Get-ChildItem -Path Cert:\LocalMachine\My*

     b. Copie la huella digital.

### Configure el certificado de CA con servicios de plugins de host de Windows

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

- Pasos*
  1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

     Por ejemplo:

     ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
     . Enlace el certificado recientemente instalado con los servicios de
     plugins del host de Windows mediante la ejecución de los siguientes
     comandos:
     ```

     ```
     > $cert = "<certificate thumbprint>"
     ```

     ```
     > $guid = [guid]::NewGuid().ToString("B")
     ```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
```

Por ejemplo:

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

### Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

### Lo que necesitará

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

### Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

## Configure SnapManager 7.x para Exchange y SnapCenter para que coexistan

Para habilitar el plugin de SnapCenter para Microsoft Exchange Server y coexistir con SnapManager para Microsoft Exchange Server, debe instalar el plugin de SnapCenter para Microsoft Exchange Server en el mismo servidor de Exchange en el que esté instalado SnapManager para Microsoft Exchange Server, deshabilitar las programaciones de SnapManager para Exchange, Y configurar programaciones y backups nuevos con el plugin de SnapCenter para Microsoft Exchange Server.

**Lo que necesitará**

- SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya se han instalado, y los backups de SnapManager para Microsoft Exchange Server se encuentran en el sistema y en el directorio SnapInfo.
- Debe haber eliminado o recuperado los backups tomados por SnapManager para Microsoft Exchange Server que ya no necesita.
- Debe haber suspendido o eliminado todas las programaciones creadas por SnapManager para Microsoft Exchange Server del programador de Windows.
- El plugin de SnapCenter para Microsoft Exchange Server y SnapManager para Microsoft Exchange Server pueden coexistir en el mismo Exchange Server, pero no es posible actualizar las instalaciones existentes de SnapManager para Microsoft Exchange Server a SnapCenter.

  SnapCenter no ofrece opciones para la actualización.

- SnapCenter no admite la restauración de las bases de datos de Exchange desde un backup de SnapManager para Microsoft Exchange Server.

  Si no desinstala SnapManager para Microsoft Exchange Server tras la instalación del plugin de SnapCenter para Microsoft Exchange Server y, más adelante, quiere restaurar un backup de SnapManager para Microsoft Exchange Server, tendrá que seguir otros pasos.

- Pasos*

  1. Empleando PowerShell en todos los nodos DAG, determine si se ha registrado VSS hardware Provider de SnapDrive para Windows: *Vssadmin list providers*

     ```
     C:\Program Files\NetApp\SnapDrive>vssadmin list providers
     vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
     tool
     (C) Copyright 2001-2013 Microsoft Corp.

     Provider name: 'Data ONTAP VSS Hardware Provider'
        Provider type: Hardware
        Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
        Version: 7. 1. 4. 6845
     ```

  2. En el directorio SnapDrive, anule el registro de VSS hardware Provider de SnapDrive para Windows: *navssprv.exe -r service –u*
  3. Compruebe que se ha eliminado VSS hardware Provider: *Vssadmin list providers*

4. Añada el host de Exchange a SnapCenter y, a continuación, instale el plugin de SnapCenter para Microsoft Windows y el plugin de SnapCenter para Microsoft Exchange Server.
5. En el directorio del plugin de SnapCenter para Microsoft Windows en todos los nodos DAG, compruebe que VSS hardware Provider esté registrado: *Vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. Detenga las programaciones de backup de SnapManager para Microsoft Exchange Server.
7. Utilizando la interfaz gráfica de usuario de SnapCenter, configure backups a petición, configure los backups programados y la configuración de retención.
8. Desinstale SnapManager para Microsoft Exchange Server.

   Si no desinstala SnapManager para Microsoft Exchange Server ahora y, más adelante, desea restaurar un backup de SnapManager para Microsoft Exchange Server:

   a. Anule el registro del plugin de SnapCenter para Microsoft Exchange Server de todos los nodos DAG: *navssprv.exe -r service -u*

   ```
   C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for
   Microsoft Windows>navssprv.exe -r service -u
   ```

   b. En el directorio *C:\Program Files\NetApp\SnapDrive*, registre SnapDrive para Windows en todos los nodos DAG: *navssprv.exe -r service -a hostname\\username -p password*

# Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

## Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

### Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

# Prepárese para la protección de datos

Antes de ejecutar una operación de protección de datos, como un backup, un clon o una restauración, debe definir una estrategia y configurar el entorno. También debe configurar SnapCenter Server para que use las tecnologías SnapMirror y SnapVault.

Para aprovechar las ventajas de las tecnologías SnapVault y SnapMirror, debe configurar e inicializar una relación de protección de datos entre el volumen de origen y el volumen de destino en el dispositivo de almacenamiento. Puede usar NetApp System Manager o la línea de comandos de la consola de almacenamiento para ejecutar estas tareas.

**Más información**

"Primeros pasos con la API DE REST"

## Requisitos previos para usar el plugin de SnapCenter para Microsoft Exchange Server

Para que se pueda usar el plugin para Exchange, el administrador de SnapCenter debe haber instalado y configurado el servidor SnapCenter y ejecutado las tareas de requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter.
- Configurar el entorno de SnapCenter añadiendo o asignando conexiones del sistema de almacenamiento y creando credenciales.

  SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada SVM compatible con SnapCenter debe tener un nombre exclusivo.

- Añadir hosts, instalar el plugin de SnapCenter para Microsoft Windows y SnapCenter el plugin para Microsoft Exchange Server, y detectar (actualizar) los recursos.
- Ejecutar el aprovisionamiento de almacenamiento en el host mediante el plugin de SnapCenter para Microsoft Windows.
- Si se usará SnapCenter Server para proteger bases de datos de Exchange que residen en un LUN de RDM de VMware, es necesario implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter. La documentación del plugin de SnapCenter para VMware vSphere tiene más información.

  Los VMDK no son compatibles.

- Mover una base de datos de Microsoft Exchange Server de un disco local a un almacenamiento compatible con las herramientas de Microsoft Exchange.

- Configure las relaciones de SnapMirror y SnapVault si quiere realizar una replicación de backup.

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para los usuarios de SnapCenter 4.3.x, la documentación del plugin de SnapCenter para VMware vSphere 4.3 tiene información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual del plugin de SnapCenter para VMware vSphere basado en Linux (formato de dispositivo virtual abierto).

"Documentación del plugin de SnapCenter para VMware vSphere"

## Uso de recursos, grupos de recursos y políticas para proteger un servidor de Exchange

Antes de usar SnapCenter, es necesariol comprender ciertos conceptos básicos vinculados con las operaciones de backup, restauración y propagación que desea ejecutar. El usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser bases de datos de buzón o grupos de disponibilidad de bases de datos (DAG) de Microsoft Exchange cuyo backup se hace desde SnapCenter.
- Un grupo de recursos de SnapCenter es un conjunto de recursos en un host o DAG de Exchange, que puede incluir un DAG completo o bases de datos individuales.

  Al realizar una operación con un grupo de recursos, esta se ejecuta en los recursos definidos en el grupo de acuerdo con la programación que se especificó para dicho grupo de recursos.

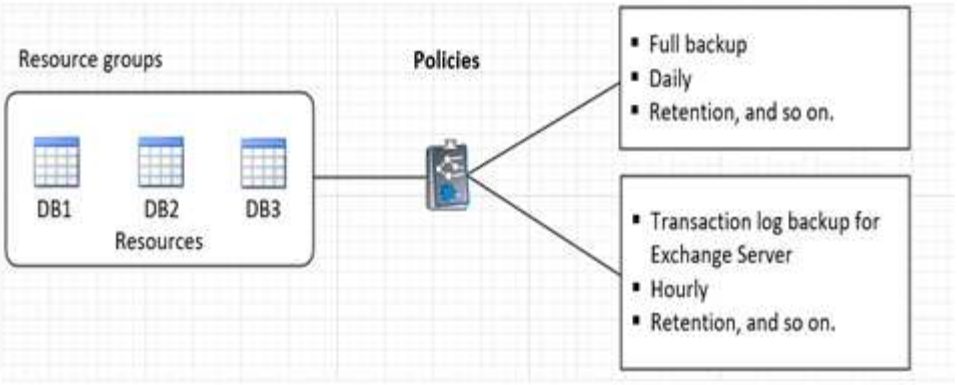
  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

  Los grupos de recursos antes se denominaban conjuntos de datos.

- Las políticas especifican la frecuencia de backup, la retención de copias, los scripts y otras características de las operaciones de protección de datos.

  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. Es posible seleccionar una política o varias al ejecutar un backup bajo demanda de un solo recurso.

Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando se crea el grupo de recursos y se vinculan las políticas, es posible configurar el grupo de recursos para que se ejecute un backup completo todos los días, y agregar una programación que ejecute un backup del registro por hora. En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:



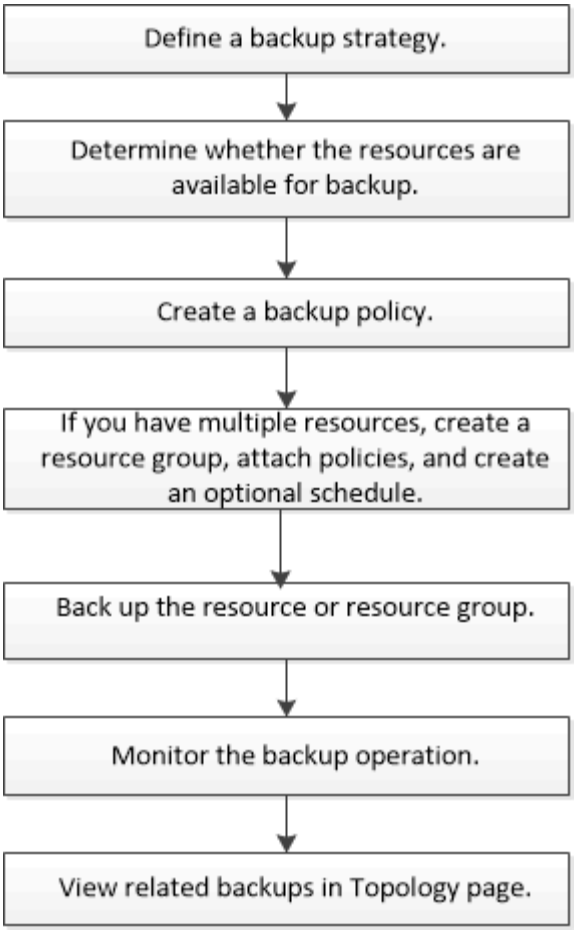

# Realice backup de recursos de Exchange

## Flujo de trabajo de backup

Cuando se instala el plugin de SnapCenter para Microsoft Exchange Server en el entorno, es posible usar SnapCenter para realizar el backup de los recursos de Exchange.

Es posible programar varios backups para que se realicen simultáneamente en diferentes servidores. No se pueden ejecutar en simultáneo operaciones de backup y restauración en el mismo recurso. No se admiten las copias de backup activas y pasivas en el mismo volumen.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:




## Verificación de la base de datos y el backup de Exchange

El plugin de SnapCenter para Microsoft Exchange Server no ofrece verificación de backups; sin embargo, es posible usar la herramienta Eseutil que se proporciona con Exchange para verificar las bases de datos y los backups de Exchange.

La herramienta Eseutil de Microsoft Exchange es una utilidad de línea de comandos que se incluye con el servidor de Exchange. La utilidad permite realizar comprobaciones de coherencia para verificar la integridad de las bases de datos y los backups de Exchange.

**Mejor práctica:** no es necesario realizar comprobaciones de consistencia en bases de datos que forman parte de una configuración DAG con al menos dos réplicas.

Para obtener más información, consulte "Documentación de Microsoft Exchange Server".

## Determine si hay recursos de Exchange disponibles para backup

Los recursos son las bases de datos y los grupos de disponibilidad de bases de datos de Exchange que se mantienen con los plugins instalados. Es posible añadir esos recursos a grupos de recursos para ejecutar tareas de protección de datos, pero primero es necesario identificar qué recursos están disponibles. Identificar los recursos disponibles también permite verificar que el plugin se haya instalado correctamente.

**Lo que necesitará**

- Es necesario completar previamente algunas tareas, como instalar SnapCenter Server, añadir hosts, crear conexiones del sistema de almacenamiento, añadir credenciales e instalar el plugin para Exchange.
- Para aprovechar las funciones del software Single Mailbox Recovery, debe haber localizado la base de datos activa en Exchange Server donde está instalado el software Single Mailbox Recovery.
- Si las bases de datos residen en LUN de RDM de VMware, es necesario implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter. La "Documentación del plugin de SnapCenter para VMware vSphere" tiene más información.

**Acerca de esta tarea**

- No se puede realizar una copia de seguridad de las bases de datos si la opción **Estado general** de la página Detalles está establecida en no disponible para la copia de seguridad. La opción **Estado general** se establece en no disponible para copia de seguridad cuando se cumple alguna de las siguientes condiciones:
  - Las bases de datos no se encuentran en un LUN de NetApp.
  - Las bases de datos no están en estado normal.

    Las bases de datos no están en estado normal cuando están en estado pendiente de montaje, desmontaje, propagación o recuperación.
- Si se posee un DAG, es posible realizar un backup de todas las bases de datos del grupo ejecutando el trabajo de backup desde el DAG.
- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **Microsoft Exchange Server** en la lista desplegable de plugins ubicada en la esquina superior izquierda de la página Recursos.
2. En la página Resources, seleccione **Database**, **Database Availability Group** o **Resource Group** en la lista desplegable **View**.

   Haga clic en Y seleccione el nombre de host y el servidor de Exchange para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.
3. Haga clic en **Actualizar recursos**.

   Los recursos recién agregados, cuyo nombre se ha cambiado o eliminado se actualizan al inventario de SnapCenter Server.

   Se muestran los recursos, junto con información como el nombre del recurso, el nombre del grupo de disponibilidad de base de datos, el servidor en el que la base de datos está activa actualmente, el servidor con copias, la hora del último backup y el estado general.

   - Si la base de datos se encuentra en un almacenamiento de terceros, se muestra Not available for backup en la columna Overall Status.

     En un DAG, si la copia de la base de datos activa se encuentra en un almacenamiento de terceros y si al menos una copia de la base de datos pasiva se encuentra en el almacenamiento de NetApp, aparece Not protected en la columna **Overall Status**.

No es posible realizar operaciones de protección de datos en una base de datos que se encuentra en un tipo de almacenamiento distinto de NetApp.

- Si la base de datos se encuentra en el almacenamiento de NetApp y no está protegida, se muestra Not protected en la columna **Overall Status**.
- Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, la interfaz de usuario muestra el mensaje Backup not run en la columna **Overall Status**.
- Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, y se activa el backup para la bases de datos, la interfaz de usuario muestra el mensaje Backup succeeded en la columna **Overall Status**.

## Crear políticas de backup para bases de datos de Exchange Server

Es posible crear una política de backup para los recursos de Exchange o los grupos de recursos antes de usar SnapCenter con el fin de realizar un backup de los recursos de Microsoft Exchange Server. También es posible crear una política de backup en el momento de crear un grupo de recursos o realizar un backup de un único recurso.

### Lo que necesitará

- Debe estar definida la estrategia de protección de datos.

  Para obtener detalles, consulte la información sobre cómo definir una estrategia de protección de datos para bases de datos de Exchange.

- Debe haberse preparado para la protección de datos completando ciertas tareas, como instalar SnapCenter, añadir hosts, identificar recursos y crear conexiones con el sistema de almacenamiento.
- Debe haber actualizado (detectado) los recursos de Exchange Server.
- Si va a replicar copias de Snapshot en un reflejo o almacén, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) para los volúmenes de origen y de destino.
- Para ejecutar los scripts de PowerShell en scripts previos y posteriores, es necesario configurar el valor de `usePowershellProcessforScripts` parámetro en true en la `web.config` archivo.

  El valor predeterminado es FALSE

### Acerca de esta tarea

Una política de backup es un conjunto de reglas que rigen cómo gestionar y conservar backups, y con qué frecuencia se realizará un backup del recurso o del grupo de recursos. Asimismo, es posible especificar la configuración de scripts. Puede especificar opciones en la política para ahorrar tiempo cuando desee reutilizarla con otro grupo de recursos.

La retención de un backup completo es específica de una política determinada. Una base de datos o un recurso que utiliza la política A con una retención de backup completo de valor 4 retiene 4 backups completos y no afecta la política B de la misma base de datos o recurso, que puede presentar una retención de valor 3 para retener 3 backups completos.

La retención de backup de registros rige para todas las políticas y se aplica a todos los backups de registros de una base de datos o registro. Por lo tanto, cuando se realiza un backup completo mediante la política B, la configuración de retención de registros afecta los backups de registros creados con la política A en la misma base de datos o el mismo recurso. De igual modo, la configuración de retención de registros de la política A afecta los backups de registros creados con la política B en la misma base de datos.

**Mejor práctica:** es mejor configurar la directiva de retención secundaria en función del número de copias de seguridad completas y de registros, en general, que desee conservar. Al configurar las políticas de retención secundarias, tenga en cuenta que cuando las bases de datos y los registros de volúmenes diferentes, cada backup puede tener tres copias de Snapshot y cuando las bases de datos y los registros están en el mismo volumen, cada backup puede tener dos copias de Snapshot.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Directivas**.
  3. Haga clic en **Nuevo**.
  4. En la página Name, escriba el nombre de la política y una descripción.
  5. En la página Backup Type, realice los siguientes pasos:
     a. Elija el tipo de backup:

| Si desea… | Realice lo siguiente… |
|---|---|
| Realice un backup de los archivos de la base de datos y de los registros de transacciones necesarios | Seleccione **copia de seguridad completa y copia de seguridad de registro**.<br><br>Se realiza un backup de las bases de datos con truncamiento de registros, y todos los registros se incluyen en el backup, incluso los truncados.<br><br>Este es el tipo de backup recomendado. |
| Realice un backup de los archivos de la base de datos y de los registros de transacciones sin confirmar | Seleccione **copia de seguridad completa**.<br><br>Se realiza un backup de las bases de datos con truncamiento de registros, y los registros acortados no se incluyen en el backup. |
| Realice un backup de todos los registros de transacciones | Seleccione **copia de seguridad de registro**.<br><br>Se realiza un backup de todos los registros de transacciones en el sistema de archivos activo y no hay truncamiento de registros.<br><br>Se crea un directorio *scebackupinfo* en el mismo disco que el registro activo. Este directorio contiene el puntero a los cambios incrementales de la base de datos de Exchange y no es equivalente a los archivos de registro completos. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Realizar un backup de todos los archivos de la base de datos y los registros de transacciones sin acortarlos | Seleccione **copia de seguridad**.<br><br>Se realiza un backup de todas las bases de datos y todos los registros y no hay truncamiento de registros. Normalmente se utiliza este tipo de backup para volver a insertar una réplica o para probar o diagnosticar un problema. |

Se debe definir el espacio requerido para los backups de registros en función de la retención de backup completo y no en la retención de último minuto (UTM).

Cree políticas de almacén independientes para registros y bases de datos cuando se trate de volúmenes de Exchange (LUN) y establezca la opción Keep (retención) para la política de registros en el doble de número para cada etiqueta que la política de base de datos, usando las mismas etiquetas. Para obtener más información, consulte: "Los backups de SnapCenter para Exchange solo conservan la mitad de las copias Snapshot en el volumen de registro de destino del almacén".

b. En la sección Database Availability Group Settings, seleccione una acción:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Realice un backup de copias activas | Seleccione esta opción para realizar un backup únicamente de las copias activas de la base de datos seleccionada.<br><br>En el caso de los grupos de disponibilidad de la base de datos (DAG), con esta opción se realiza un backup solo de las copias activas de todas las bases de datos en el DAG.<br><br>Las copias pasivas no se incluyen en el backup. |
| Realizar un backup de las copias en los servidores que se seleccionarán en el momento de crear el trabajo de backup | Seleccione esta opción para realizar un backup de cualquier copia de las bases de datos en los servidores seleccionados, ya sean activas o pasivas.<br><br>En el caso de los DAG, con esta opción se realiza un backup tanto de las copias activas como pasivas de todas las bases de datos en los servidores seleccionados. |

En las configuraciones de clúster, los backups se conservan en cada nodo del clúster según la configuración de retención establecida en la política. Si cambia el nodo propietario del clúster, se conservarán las copias de seguridad del nodo propietario anterior. La retención solo se aplica a nivel de nodo.

c. En la sección frecuencia de programación, seleccione uno o más tipos de frecuencia: **A petición**, **hora**, **Diario**, **Semanal** y **Mensual**.

Es posible especificar el cronograma (fecha de inicio y de finalización) para las operaciones de backup a la vez que se crea un grupo de recursos. De este modo, se pueden crear grupos de recursos que comparten la misma política y frecuencia de backup, pero se pueden asignar diferentes programaciones de backup a cada política.

Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

6. En la página Retention, configure los ajustes de retención.

Las opciones que se muestren dependerán del tipo de backup y de frecuencia previamente seleccionados.

El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.

Debe establecer el número de retención en 2 o un valor más alto si tiene pensado habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino.

a. En la sección Log backups retention settings, seleccione una de las siguientes opciones:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Retener únicamente una cantidad específica de backups de registros | Seleccione **Number of full backups for which logs are retained** y especifique la cantidad de backups completos para la cual desea definir una capacidad de restauración de último minuto.<br><br>La retención de último minuto (UTM) se aplica al backup de registros creado mediante un backup completo o un backup de registros. Por ejemplo, si la configuración de retención UTM se configura para retener los backups de registros de los últimos 5 backups completos, se conservan los backups de registros de los últimos 5 backups completos.<br><br>Las carpetas de registro creadas como parte de los backups completos y de registros se eliminan automáticamente como parte de UTM. No es posible eliminar las carpetas de registro manualmente. Por ejemplo, si la configuración de retención de backup completo o completo y el backup de registros se establece en 1 mes y la retención UTM se establece en 10 días, la carpeta de registro creada como parte de estos backups se eliminará según UTM. Como resultado, solo habrá 10 días de carpetas de registro y todos los demás backups se marcan para una restauración a un momento específico.<br><br>Es posible configurar el valor de retención UTM como 0, si no desea realizar una restauración de último minuto. Esto habilitará la operación de restauración a un momento específico.<br><br>**Mejor práctica:** es mejor que la configuración sea igual a la configuración de copias Snapshot totales (copias de seguridad completas) en la sección Configuración de retención de copias de seguridad completas. De este modo se garantiza que se conservan los archivos de registro para cada backup completo. |
| Retener las copias de backup por una cantidad determinada de días | Seleccione la opción **Keep log backups for last** y especifique el número de días que se conservarán las copias de seguridad de registro.<br><br>Se conservan los backups de registros por la cantidad de días de backups completos. |

Si seleccionó **Log backup** como tipo de copia de seguridad, las copias de seguridad de registros se conservan como parte de la configuración de retención de último minuto para las copias de seguridad completas.

b. En la sección Full backup retention settings, seleccione una de las siguientes opciones para backups a petición y, a continuación, seleccione una opción para backups completos:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Retener únicamente una cantidad específica de copias de Snapshot | Si desea especificar el número de copias de seguridad completas que se conservarán, seleccione la opción **total Snapshot copies to keep** y especifique el número de copias de Snapshot (copias de seguridad completas) que se retendrán.<br><br>Si se supera la cantidad especificada de backups completos, se eliminarán los backups completos que exceden dicha cantidad empezando por las copias más antiguas. |
| Retener los backups completos por una cantidad determinada de días | Seleccione la opción **Keep Snapshot copies for** y especifique la cantidad de días que se conservarán las copias de Snapshot (copias de seguridad completas). |

Si se dispone de una base de datos que solo tiene backups de registros y ningún backup completo en un host de una configuración de DAG, los backups de registros se retienen de las siguientes maneras:

- De forma predeterminada, SnapCenter busca el backup completo más antiguo de la base de datos en todos los otros hosts del DAG y elimina todos los backups de registros de este host que se realizaron antes del backup completo.
- Para anular este comportamiento de retención predeterminada en una base de datos en un host de un DAG que solo presenta backups de registros, se puede añadir la clave * MaxLogBackupOnlyCountWithoutFullBackup* en el archivo *C:\Program Files\NetApp\SnapCenter WebApp\web.config*.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

En el ejemplo, el valor 10 indica que se conservan hasta 10 backups de registros en el host.

7. En la página Replication, seleccione una o ambas de las siguientes opciones de replicación secundaria:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Actualizar SnapMirror tras crear una copia Snapshot local | Seleccione esta opción para mantener copias de SnapMirror de conjuntos de backups en otro volumen (SnapMirror). |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Actualizar SnapVault después de crear una copia Snapshot local | Seleccione esta opción para realizar una replicación de backup de disco a disco. |
| Etiqueta de la política secundaria | Seleccione una etiqueta de Snapshot.<br><br>Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta.<br><br>Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria. |
| Número de reintentos con error | Introduzca el número de intentos de replicación que deben producirse antes de que se interrumpa el proceso. |

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

8. En la página Script, introduzca la ruta y los argumentos del script previo o script posterior que se deben ejecutar antes o después de la operación de backup, según corresponda.
   - Los argumentos de copia de seguridad del script incluyen "'$Database'" y "'$ServerInstance'".
   - Los argumentos de copia de seguridad de PostScript incluyen «»$Database», «»$ServerInstance», «»$BackupName», «»$LogDirectory» y «»$LogSnapshot».

     Es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear grupos de recursos y añadir políticas para Exchange Server

Un grupo de recursos es necesario para cualquier trabajo de protección de datos. También deben añadir una o varias políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que se quiere realizar y la programación de protección.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento de Microsoft Exchange Server en la lista.
2. En la página Resources, seleccione **Database** en la lista **View**.

   Si recientemente ha agregado un recurso a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recién añadido.

3. Haga clic en **Nuevo grupo de recursos**.
4. En la página Name, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba el nombre del grupo de recursos.<br>El nombre del grupo de recursos no debe superar los 250 caracteres. |
| Etiquetas | Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.<br>Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta. |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Opcional: Escriba un nombre de copia de Snapshot personalizado y su formato.<br>Por ejemplo, *customtext_resourcegroup_policy_hostname* o *resourcegroup_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |

5. En la página Resources, realice los siguientes pasos:

   a. Seleccione el tipo de recurso y el DAG en las listas desplegables para filtrar la lista de recursos disponibles.

      Si recientemente añadió recursos, aparecerán en la lista Available Resources solo después de actualizar la lista de recursos.

   En las secciones Available Resources y Selected Resources, el nombre de la base de datos se muestra con el nombre de host. Este nombre de host solo indica que la base de datos está activa en ese host específico y que puede no asumir un backup en este host. Debe seleccionar uno o más servidores de copia de seguridad de la opción de selección del servidor, donde desea realizar la copia de seguridad en caso de que haya seleccionado la opción **copia de seguridad de copias en servidores para seleccionar en el tiempo de creación del trabajo de copia de seguridad** de la directiva.

a. Escriba el nombre del recurso en el cuadro de texto de búsqueda o desplácese para ubicar un recurso.

b. Para mover los recursos de la sección Available Resources a la sección Selected Resources, realice uno de los siguientes pasos:

- Seleccione **Autoselect all resources on same Storage volume** para mover todos los recursos del mismo volumen a la sección Selected Resources.
- Seleccione los recursos de la sección Available Resources y, a continuación, haga clic en la flecha derecha para mover estos elementos a la sección Selected Resources.

  Los grupos de recursos de SnapCenter para Microsoft Exchange Server no pueden tener más de 30 bases de datos por copia de Snapshot. Si hay más de 30 bases de datos en un grupo de recursos, se crea una segunda copia de Snapshot para las bases de datos adicionales. Por lo tanto, se crean 2 subtrabajos en la tarea de copia de seguridad principal. Para los backups que tienen replicación secundaria, mientras que la actualización de SnapMirror o SnapVault está en curso, es posible que haya escenarios en los que la actualización de ambos subtrabajos se superponga. La tarea de backup principal se mantiene en ejecución permanente incluso si los registros indican que la tarea se ha completado.

6. En la página Policies, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.

También puede crear una directiva haciendo clic en + .

Si una directiva contiene la opción **copia de seguridad de copias en los servidores que se van a seleccionar en tiempo de creación de trabajos de copia de seguridad**, se muestra una opción de selección de servidor para seleccionar uno o más servidores. La opción de selección del servidor incluirá únicamente el servidor donde la base de datos seleccionada esté en el almacenamiento de NetApp.

En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

b. En la sección Configure schedules for selected policies, haga clic en + En la columna **Configurar horarios** de la directiva para la que desea configurar la programación.

c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación especificando la fecha de inicio, la fecha de caducidad y la frecuencia y, a continuación, haga clic en **Aceptar**.

Debe hacerlo con cada frecuencia que figure en la política. Los horarios configurados se enumeran en la columna **programas aplicados** de la sección Configurar programaciones para directivas seleccionadas.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

7. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así

como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

Para habilitar la notificación por correo electrónico, debe tener especificados los detalles del servidor SNMP ya sea mediante la GUI o el comando de PowerShell `Set-SmSmtpServer`.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Realizar backup de bases de datos de Exchange

Si una base de datos no pertenece a ningún grupo de recursos, es posible realizar backups de la base de datos o del grupo de disponibilidad de base de datos desde la página Resources.

### Lo que necesitará

- Debe tener creada una política de backup.
- Se debe haber asignado el agregado que usa la operación de backup a la máquina virtual de almacenamiento usada por la base de datos.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, el rol asignado al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Si desea realizar backup de una base de datos o un grupo de disponibilidad de base de datos que tenga copia de base de datos activa/pasiva en un almacenamiento de NetApp y de otro tipo, Y ha seleccionado la opción **copia de seguridad de copias activas** o **copia de seguridad de copias en servidores que se seleccionarán durante la creación de trabajos de copia de seguridad** en la directiva; a continuación, los trabajos de copia de seguridad irán al estado de advertencia. El backup tendrá éxito con una copia de base de datos activa/pasiva en el almacenamiento de NetApp y el backup generará un error cuando se copie una base de datos activa/pasiva en un sistema de almacenamiento de otro fabricante.

  **Mejor práctica:** no ejecute copias de seguridad de bases de datos activas y pasivas al mismo tiempo. Se puede producir una condición de carrera y uno de los backups puede fallar.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el **plug-in de Microsoft Exchange Server** en la lista.
2. En la página Resources, seleccione **Database** o **Database Availability Group** en la lista **View**.

   En la página Resources, el Icono indica que la base de datos está en un almacenamiento de otros proveedores.

   En un DAG, si una copia activa de la base de datos se encuentra en un almacenamiento de terceros y al menos una copia pasiva de ella reside en un almacenamiento de NetApp, puede proteger la base de datos.

Haga clic en y luego seleccione el nombre de host y el tipo de base de datos para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.

- Para realizar el backup de una base de datos, se debe hacer clic en el nombre de la base de datos.
  i. Si aparece la vista Topology, haga clic en **Protect**.
  ii. Si aparece el Asistente para bases de datos - proteger recursos, continúe con el paso 3.
- Para realizar backup de un grupo de disponibilidad de base de datos, se debe hacer clic en el nombre del grupo.

3. Para especificar un nombre personalizado para la copia de Snapshot, en la página Resources, active la casilla de verificación **usar formato de nombre personalizado para copia de Snapshot** y, a continuación, escriba el formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.

4. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

   También puede crear una directiva haciendo clic en .

   Si una directiva contiene la opción **copia de seguridad de copias en los servidores que se van a seleccionar en tiempo de creación de trabajos de copia de seguridad**, se muestra una opción de selección de servidor para seleccionar uno o más servidores. La opción de selección del servidor incluirá únicamente el servidor donde la base de datos seleccionada esté en un sistema de almacenamiento NetApp.

   En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   b. Haga clic en En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

   c. En la ventana Add schedules for policy *policy_name*, configure la programación y haga clic en **OK**.

   Donde, *policy_name* es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

5. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea asociar el informe de la operación de backup ejecutada en el recurso, seleccione **Attach Job Report**.

Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de la base de datos.

2. Haga clic en **copia de seguridad ahora**.
3. En la página Backup, realice los siguientes pasos:
   a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
4. Supervise el progreso del backup haciendo doble clic en el trabajo en el panel Activity en la parte inferior de la página para que se muestre la página Job Details.
   - En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

     Para obtener más información, consulte: "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"

   - Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup.

     Para aumentar el tamaño de pila de Java, busque el archivo de script */opt/netapp/init_scripts/svservice*. En ese script, el comando *do_start method* inicia el servicio de complemento de VMware de SnapCenter. Actualice este comando a lo siguiente: *Java -jar -Xmx8192M -Xms4096M*

## Realizar backup de grupos de recursos de Exchange

Un grupo de recursos es un conjunto de recursos en un host o DAG de Exchange, y puede incluir un DAG completo o bases de datos individuales. Puede realizar backups de los grupos de recursos desde la página Resources.

### Lo que necesitará

- Debe tener creado un grupo de recursos con una política anexada.
- Asignó el agregado que utiliza la operación de backup a la SVM que utiliza la base de datos.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, el rol asignado al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, es posible que la operación de backup en algunos hosts comience tarde debido a problemas de red. Debe configurar el valor de

`MaxRetryForUninitializedHosts` pulg `web.config` mediante el uso de `Set-SmConfigSettings` Cmdlet de PowerShell.

- En un grupo de recursos, si incluye una base de datos o un grupo de disponibilidad de base de datos con copia de base de datos activa/pasiva en un almacenamiento de NetApp y de terceros, y ha seleccionado **realizar backup de copias activas** o **realizar backup de copias en los servidores que se seleccionarán durante la opción de tiempo de creación del trabajo de backup** en la política, entonces, los trabajos de backup pasan a estado de advertencia.

  El backup tendrá éxito con una copia de base de datos activa/pasiva en el almacenamiento de NetApp y el backup generará un error cuando se copie una base de datos activa/pasiva en un sistema de almacenamiento de otro fabricante.

**Acerca de esta tarea**

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el **plug-in de Microsoft Exchange Server** en la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Puede buscar el grupo de recursos escribiendo el nombre en el cuadro de búsqueda o haciendo clic en y, a continuación, seleccionar la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso del backup haciendo doble clic en el trabajo en el panel Activity en la parte inferior de la página para que se muestre la página Job Details.

## Cree una conexión de sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para Exchange Server

Es posible crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar cmdlets de PowerShell para realizar backups y restaurar.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

  No debe haber instalaciones de complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

  SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de datos única.

- Pasos*

1. Inicie una sesión de conexión de PowerShell mediante el `Open-SmConnection` cmdlet.

   En este ejemplo, se abre una sesión de PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Cree una nueva conexión con el sistema de almacenamiento mediante el `Add-SmStorageConnection` cmdlet.

   En este ejemplo, se crea una nueva conexión con el sistema de almacenamiento:

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Cree una nueva cuenta Run as con el `Add-Credential` cmdlet.

   En este ejemplo, se crea una nueva cuenta Run as denominada "ExchangeAdmin" con credenciales de Windows:

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
-Credential sddev\administrator
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Realizar backup de recursos de Exchange con cmdlets de PowerShell

La operación de backup de una base de datos de servidor de Exchange implica establecer una conexión con SnapCenter Server, detectar la base de datos de servidor

de Exchange, añadir una política, crear un grupo de recursos de backup, realizar el backup y ver el estado del backup.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe añadir la conexión con el sistema de almacenamiento y crear una credencial.
- Es necesario haber añadido los hosts y detectado los recursos.

> El plugin para Exchange no es compatible con operaciones de clonado; por lo tanto, el parámetro CloneType para el cmdlet Add-SmPolicy no es compatible con el plugin para Exchange

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Cree una política de backup mediante el cmdlet Add-SmPolicy.

   Este ejemplo crea una nueva política de backup con un backup completo y un backup de registros de Exchange:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

   Este ejemplo crea una nueva política de backup con un backup completo cada hora y un backup de registros de Exchange:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

   Este ejemplo crea una nueva política de backup para incluir solo los registros de Exchange:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Para detectar recursos de host se usa el cmdlet Get-SmResources.

   Este ejemplo detecta los recursos del plugin para Microsoft Exchange Server en el host especificado:

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

4. Añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

   Este ejemplo crea un nuevo grupo de recursos de backup de base de datos de servidor de Exchange con la política y los recursos especificados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log
_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

   Este ejemplo crea un nuevo grupo de recursos de backup de DAG de Exchange con la política y los recursos especificados:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log
_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

   En este ejemplo, se crea un nuevo backup en el almacenamiento secundario:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Consulte el estado del trabajo de backup mediante el cmdlet Get-SmBackupReport.

   Este ejemplo muestra un informe con un resumen de todos los trabajos realizados en la fecha

especificada:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Este ejemplo muestra un informe de resumen de tarea para un ID de tarea:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, consulte "Guía de referencia de cmdlets de SnapCenter Software".

## Supervisar las operaciones de backup

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Monitor, haga clic en **Jobs**.
  3. En la página Jobs, realice los siguientes pasos:
     a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
     b. Especifique las fechas de inicio y finalización.
     c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
     d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
     e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
  4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

Aunque el estado del trabajo de backup indique ✔, al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

**Supervise las operaciones en el panel Activity**

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también muestra información sobre la operación de propagación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

     Al hacer clic en una de las operaciones, se muestran sus detalles en la página Job Details.

## Cancelar las operaciones de backup de la base de datos de Exchange

Es posible cancelar las operaciones de backup que se encuentran en cola.

**Lo que necesitará**

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o el panel **Activity**.
- No es posible cancelar una operación de backup en ejecución.
- Es posible utilizar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de backup.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.
- Pasos*
  1. Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | a. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**. |
| Panel de actividades | a. Tras iniciar la operación de backup, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>b. Seleccione la operación.<br>c. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

Se cancela la operación y el recurso se revierte al estado anterior.

## Quitar los backups de Exchange mediante el cmdlet de PowerShell

Es posible usar el cmdlet Remove-SmBackup para eliminar backups de Exchange si ya no es necesario conservarlos para otras operaciones de protección de datos.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

2. Elimine uno o varios backups con el `Remove-SmBackup` cmdlet.

   Este ejemplo elimina dos backups según sus ID de backup:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

## Consulte los backups de Exchange en la página Topology

Al preparar el backup de un recurso, puede ser útil ver una representación gráfica de todos los backups del almacenamiento principal y secundario.

### Acerca de esta tarea

En la página Topology, es posible ver todos los backups disponibles para el recurso o el grupo de recursos seleccionado. Es posible ver los detalles de esos backups y, luego, seleccionarlos para ejecutar operaciones de protección de datos.

Puede revisar el siguiente icono en la vista gestionar copias para determinar si los backups están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

- muestra la cantidad de backups disponibles en el almacenamiento principal.
- Muestra la cantidad de backups que estan copiados en el almacenamiento secundario mediante SnapMirror.
- Muestra la cantidad de backups que se replican en el almacenamiento secundario mediante la tecnología SnapVault.
  - La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario.

    Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

| **Mejor práctica:** para asegurarse de que se muestra el número correcto de copias de seguridad replicadas, le recomendamos que actualice la topología. |
|---|

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione la base de datos, el recurso o el grupo de recursos en la lista desplegable **View**.
3. Se debe seleccionar el recurso desde la vista de detalles de la base de datos o desde la vista de detalles del grupo de recursos.

   Si el recurso está protegido, se muestra la página Topology del recurso seleccionado.

4. En la sección Summary Card, se muestra un resumen de la cantidad de backups disponibles en el almacenamiento principal y secundario.

   En la sección Summary Card, se muestra la cantidad total de backups y de backups de registros.

Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento

preciso.

1. En la vista Administrar copias, haga clic en **copias de seguridad** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad.

   Estos detalles se muestran en forma de tabla.

2. Seleccione el backup en la tabla y haga clic en los iconos de protección de datos para realizar operaciones de restauración, cambio de nombre y eliminación.

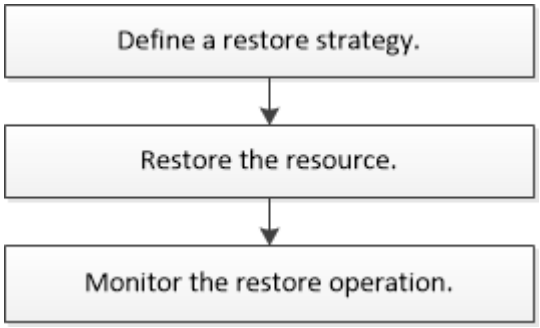
   Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre. La configuración de retención de ONTAP gestiona la eliminación de copias Snapshot.

# Restaurar recursos de Exchange

## Restaure el flujo de trabajo

SnapCenter permite restaurar bases de datos de Exchange mediante la restauración de uno o varios backups en el sistema de archivos activo.

En el siguiente flujo de trabajo, se muestra la secuencia que debe seguirse para ejecutar las operaciones de restauración de bases de datos de Exchange:




También es posible usar los cmdlets de PowerShell manualmente o en scripts para ejecutar las operaciones de backup y restauración. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software".

## Requisitos para restaurar una base de datos de Exchange

Para poder restaurar una base de datos de servidor de Exchange desde un backup del plugin de SnapCenter para Microsoft Exchange Server, se deben cumplir varios requisitos.

- El servidor de Exchange debe estar en línea y en ejecución para poder restaurar una base de datos.
- Las bases de datos deben encontrarse en el servidor de Exchange.

  No se admite la restauración de bases de datos eliminadas.

- Las programaciones de SnapCenter para la base de datos deben estar suspendidas.

- El servidor de SnapCenter y el host del plugin de SnapCenter para Microsoft Exchange Server deben estar conectados al almacenamiento primario y secundario que contiene los backups que desea restaurar.

## Restaurar bases de datos de Exchange

Es posible usar SnapCenter para restaurar bases de datos de Exchange incluidas en backups.

### Lo que necesitará

- Es necesario tener en cuenta el backup de los grupos de recursos, la base de datos o los DAG.
- Cuando la base de datos de Exchange se migra a otra ubicación, la operación de restauración no funciona con backups antiguos.
- Si va a replicar copias de Snapshot en un reflejo o almacén, el administrador de SnapCenter debe haberle asignado las SVM correspondientes a los volúmenes de origen y destino.
- En un DAG, si una copia de la base de datos activa se encuentra en un almacenamiento de terceros y desea restaurar desde el backup de copia de base de datos pasiva que se encuentra en un almacenamiento de NetApp, hacer que la copia pasiva (almacenamiento de NetApp) sea una copia activa, actualizar los recursos y realizar la operación de restauración.

  Ejecute el `Move-ActiveMailboxDatabase` comando para realizar la copia pasiva de la base de datos como copia activa de la base de datos.

  La "Documentación de Microsoft" contiene información acerca de este comando.

### Acerca de esta tarea

- Cuando se realiza una operación de restauración en una base de datos, la base de datos se monta de nuevo en el mismo host y no se crea ningún volumen nuevo.
- Los backups DE DAG deben restaurarse desde bases de datos individuales.
- No se admite la restauración de disco completo si hay otros archivos además del archivo de base de datos de Exchange (.edb).

  El plugin para Exchange no realiza una restauración completa en un disco si el disco contiene archivos de Exchange como los que se utilizan para la replicación. Cuando una restauración completa puede afectar la funcionalidad de Exchange, el plugin para Exchange realiza una sola operación de restauración de archivos.

- El plugin para Exchange no puede restaurar unidades cifradas BitLocker.
- Pasos*

  1. En el panel de navegación izquierdo, haga clic en **Recursos** en la esquina superior izquierda de la página Recursos.
  2. Seleccione el plugin para servidor de Exchange de la lista desplegable.
  3. En la página Resources, seleccione **Database** en la lista View.
  4. Seleccione la base de datos de la lista.
  5. En la vista Manage Copies, seleccione **copias de seguridad**, en la tabla Primary backups y, a continuación, haga clic en .

6. En la página Options, se debe seleccionar una de las siguientes opciones de backup:

| Opción | Descripción |
| --- | --- |
| Todos los backups de registros | Seleccione **todas las copias de seguridad de registros** para ejecutar la operación de restauración de copia de seguridad de último minuto para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa. |
| Mediante backups de registros hasta que | Seleccione **by log backups until** para realizar una operación de restauración a un momento específico, que restaura la base de datos en función de las copias de seguridad de registros hasta el registro seleccionado.<br>El número de registros que se muestran en la lista desplegable se basa en UTM. Por ejemplo, si la retención de backup completo es 5 y la retención UTM es 3, la cantidad de backups de registros disponibles es 5, pero en la lista desplegable solo 3 registros se mostrarán para realizar la operación de restauración. |
| Por fecha específica hasta | Seleccione **por fecha específica hasta** para especificar la fecha y hora hasta la que se aplican los registros de transacciones a la base de datos restaurada. Esta operación de restauración a un momento específico restaura las entradas del registro de transacciones que se registraron hasta el último backup en la fecha y hora especificadas. |
| Ninguno | Elija **Ninguno** cuando necesite restaurar sólo la copia de seguridad completa sin ninguna copia de seguridad de registro. |

Es posible realizar una de las siguientes acciones:

- **Recover and Mount database after restore** - esta opción está seleccionada de forma predeterminada.
- **No verifique la integridad de los registros de transacciones en la copia de seguridad antes de la restauración** - de forma predeterminada, SnapCenter verifica la integridad de los registros de transacciones en una copia de seguridad antes de realizar una operación de restauración.

  **Mejor práctica:** no debe seleccionar esta opción.

7. En la página Script, se deben introducir la ruta y los argumentos del script previo o posterior que se

ejecutará antes o después de la operación de restauración.

Los argumentos de script previo de restauración incluyen $Database y $ServerInstance.

Los argumentos de postscript de restauración incluyen $Database, $ServerInstance, $BackupName, $LogDirectory y $TargetServerInstance.

Es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

1. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo.

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.
3. Para ver el estado de la tarea de restauración, se debe expandir el panel Activity en la parte inferior de la página.

   Debe supervisar el proceso de restauración mediante la página **Monitor** > **Jobs**.

Cuando se restaura una base de datos activa desde un backup, la base de datos pasiva puede entrar en estado de suspensión o error si hay un desfase entre la réplica y la base de datos activa.

El cambio de estado puede ocurrir cuando la cadena de registros de la base de datos activa se divide y comienza una nueva línea, lo cual interrumpe la replicación. El servidor de Exchange intenta reparar la réplica, pero si no puede hacerlo, después de la restauración, debe crear un backup nuevo y luego reinicializar la réplica.

## Recuperación granular de correos y buzones de correo

El software Single Mailbox Recovery (SMBR) le permite restaurar y recuperar mensajes de correo electrónico o buzones en lugar de la base de datos completa de Exchange.

La restauración de bases de datos completas sólo para recuperar un correo individual consume mucho tiempo y recursos. SMBR le ayuda a recuperar rápidamente los mensajes de correo electrónico creando una copia de clon de la Snapshot y, a continuación, usando las API de Microsoft para montar el buzón en SMBR. Para obtener información sobre cómo utilizar SMBR, consulte "Guía de administración de SMBR".

Si quiere más información sobre SMBR, consulte lo siguiente:

- "Cómo restaurar manualmente un solo elemento con SMBR (también se aplica a las restauraciones de Ontrack Power Control)"
- "Cómo restaurar desde el almacenamiento secundario en SMBR con SnapCenter"
- "Recuperación de Microsoft Exchange Mail desde SnapVault mediante SMBR"

## Restaurar una base de datos de servidor de Exchange desde un almacenamiento secundario

Es posible restaurar una base de datos de Exchange Server con backup a partir de un almacenamiento secundario (reflejo o almacén).

Debe haber replicado las copias de Snapshot a desde el almacenamiento principal hasta un almacenamiento secundario.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **plug-in de Microsoft Exchange Server** en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista desplegable **View**.
3. Seleccione la base de datos o el grupo de recursos.

   Se muestra la página de topología de la base de datos o el grupo de recursos.

4. En la sección Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento secundario (mirror o vault).
5. Seleccione el backup en la lista y haga clic en .
6. En la página Location, elija el volumen de destino para restaurar el recurso seleccionado.
7. Complete el asistente Restaurar, revise el resumen y, a continuación, haga clic en **Finalizar**.

## Restaurar recursos de Exchange mediante cmdlets de PowerShell

La restauración de una base de datos de Exchange incluye el inicio de una sesión de conexión con el servidor SnapCenter, el listado de los backups y la recuperación de información de los backups, y la restauración de un backup.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

- Pasos*

1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado mediante el `Open-SmConnection` cmdlet.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
   ```

2. Recupere la información sobre uno o varios de los backups que desea restaurar mediante el `Get-SmBackup` cmdlet.

   Este ejemplo muestra información sobre todos los backups disponibles:

```
PS C:\> Get-SmBackup

BackupId                        BackupName
BackupTime                      BackupType
--------                        ----------
----------                      ----------
341                             ResourceGroup_36304978_UTM... 12/8/2017
4:13:24 PM          Full Backup
342                             ResourceGroup_36304978_UTM... 12/8/2017
4:16:23 PM          Full Backup
355                             ResourceGroup_06140588_UTM... 12/8/2017
6:32:36 PM          Log Backup
356                             ResourceGroup_06140588_UTM... 12/8/2017
6:36:20 PM          Full Backup
```

3. Restaure datos del backup mediante la `Restore-SmBackup` cmdlet.

   Este ejemplo restaura un backup de último minuto:

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

   Este ejemplo restaura un backup de momento específico:

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

   Este ejemplo restaura un backup en el almacenamiento secundario al argumento primario:

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BackupId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

   La `-archive` parámetro permite especificar los volúmenes primario y secundario que se desean usar para la restauración.

La `-IsRecoverMount:$true` parámetro permite montar la base de datos después de la restauración.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de

referencia de cmdlets de SnapCenter Software".

## Propagación de una réplica pasiva del nodo de Exchange

Si necesita realimentar una copia de réplica, por ejemplo, cuando una copia está dañada, puede realimentar el backup más reciente con la función de propagación en SnapCenter.

- Debe utilizar SnapCenter Server 4.1 o una versión posterior, y el plugin para Exchange 4.1 o una versión posterior.

  Las versiones de SnapCenter anteriores a 4.1 no admiten volver a insertar una réplica.

- Debe haber creado un backup de la base de datos que desea realimentar.

**Práctica recomendada:** para evitar el retraso entre nodos, recomendamos crear una nueva copia de seguridad antes de realizar una operación de propagación o elegir el host con la última copia de seguridad.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **plug-in de Microsoft Exchange Server** en la lista.
2. En la página **Recursos**, seleccione la opción adecuada en la lista Ver:

| Opción | Descripción |
|---|---|
| Para realimentar una sola base de datos | Seleccione **base de datos** en la lista View. |
| Para realimentar bases de datos en un DAG | Seleccione **Grupo de disponibilidad de base de datos** en la lista View. |

3. Seleccione el recurso que desea propagar.
4. En la página **Administrar copias**, haga clic en **propagación**.
5. En la lista de copias de bases de datos que no son saludables del asistente de propagación, seleccione la que desea propagar y haga clic en **Siguiente**.
6. En la ventana Host, seleccione el host con el backup del que desea reinicializar y haga clic en **Siguiente**.
7. En la página **Script**, introduzca la ruta de acceso y los argumentos del script previo o posterior que se deben ejecutar antes o después de la operación de propagación, respectivamente.

   Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

8. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

10. Para ver el estado de la tarea, se debe expandir el panel Activity en la parte inferior de la página.

> La operación de propagación no es compatible si la copia de base de datos pasiva reside en un almacenamiento de terceros.

## Repropagación de una réplica mediante cmdlets de PowerShell para base de datos de Exchange

Puede usar cmdlets de PowerShell para restaurar una réplica en mal estado mediante la copia más reciente del mismo host o la copia más reciente de un host alternativo.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado mediante el `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Realimentar la base de datos mediante el `reseed-SmDagReplicaCopy` cmdlet.

   En este ejemplo se reactiva la copia fallida de la base de datos denominada execdb en el host "mva-rx200.netapp.com" utilizando la última copia de seguridad en ese host.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   En este ejemplo se reactiva la copia fallida de la base de datos denominada execdb utilizando la última copia de seguridad de la base de datos (producción/copia) en un host alternativo "mva-rx201.netapp.com."

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

## Supervisar operaciones de restauración

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

### Acerca de esta tarea

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación

de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

## Cancelar las operaciones de restauración para base de datos de Exchange

Es posible cancelar los trabajos de restauración que se encuentran en cola.

Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.

**Acerca de esta tarea**

- Es posible cancelar una operación de restauración en cola desde la página Monitor o el panel Activity.
- No se puede cancelar una operación de restauración en ejecución.

- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está desactivado para operaciones de restauración que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de restauración en cola de otros miembros mientras utiliza esa función.

**Paso**

Ejecute una de las siguientes acciones:

| Del… | Acción |
| --- | --- |
| Página Monitor | 1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>2. Seleccione el trabajo y haga clic en **Cancelar trabajo**. |
| Panel de actividades | 1. Después de iniciar la operación de restauración, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>2. Seleccione la operación.<br>3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

# Proteger aplicaciones personalizadas

## Plugins personalizados de SnapCenter

### Información general sobre los plugins personalizados de SnapCenter

Es posible crear plugins personalizados para las aplicaciones que se usan y emplear SnapCenter para el backup, la restauración o la clonado de tales aplicaciones. Al igual que otros plugins de SnapCenter, los plugins personalizados funcionan como componentes del host en el software SnapCenter de NetApp y permiten la protección de datos para aplicaciones y la gestión de recursos.

Cuando se instalan plugins personalizados, es posible usar SnapCenter con la tecnología NetApp SnapMirror para crear mirrors de conjuntos de backups en otro volumen, y la tecnología NetApp SnapVault para la replicación de backup de disco a disco. Los plugins personalizados se pueden utilizar tanto en entornos de Windows como de Linux.

> La interfaz de línea de comandos no admite los comandos de los plugins personalizados de SnapCenter SnapCenter.

NetApp incluye plugins personalizados de MySQL y DB2 con SnapCenter Software 2.0 y versiones posteriores, y un plugin personalizado para MongoDB a partir de la versión 3.0. Estos plugins pueden descargarse del "Almacén de automatización del almacenamiento de NetApp".

> Los plugins personalizados de MySQL, DB2 y MongoDB reciben soporte exclusivamente a través de las comunidades de NetApp.

Para crear sus propios plugins personalizados, consulte "Desarrolle un complemento para la aplicación".

### Tareas que pueden llevarse a cabo con los plugins personalizados de SnapCenter

Los plugins personalizados de SnapCenter sirven para las operaciones de protección de datos.

- Añadir recursos como bases de datos, instancias, documentos o espacios de tablas.
- Crear backups.
- Restaurar desde backups.
- Clonar backups.
- Programar operaciones de backup.
- Supervisar operaciones de backup, de restauración y de clonado.
- Ver informes para operaciones de backup, restauración y clonado.

### Funciones de los plugins personalizados de SnapCenter

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con los plugins personalizados, se utiliza la

interfaz gráfica de usuario de SnapCenter.

- **Interfaz gráfica de usuario unificada**

  La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar operaciones de backup, restauración, recuperación y clonado consistentes entre plugins, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins.

- **Administración central automatizada**

  Es posible programar operaciones de backup, configurar la retención de backup basado en políticas y realizar operaciones de restauración. También es posible supervisar de manera proactiva el entorno configurando SnapCenter para que envíe alertas por correo electrónico.

- **Tecnología de copia snapshot de NetApp** no disruptiva

  SnapCenter utiliza la tecnología de copia de Snapshot de NetApp con los plugins personalizados de SnapCenter para realizar backups de recursos. Las copias de Snapshot consumen un espacio de almacenamiento mínimo.

Usar la función de los plugins personalizados ofrece además los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración y clonado
- Seguridad compatible con RBAC y delegación de roles centralizada

  También es posible configurar las credenciales para que los usuarios de SnapCenter autorizados tengan permisos en el nivel de las aplicaciones.

- Creación de copias de recursos con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

  Se requiere una licencia de FlexClone en el sistema de almacenamiento donde desea crear el clon.

- Compatibilidad con la función de copia de Snapshot de grupo de consistencia de ONTAP como parte de la creación de backups.
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de recursos

  En una sola operación se consolidan copias de Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear copias de Snapshot con comandos externos
- Capacidad para crear copias de Snapshot consistentes con el sistema de archivos en entornos Windows

## Tipos de almacenamiento compatibles con los plugins personalizados de SnapCenter

SnapCenter admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Debe comprobar la compatibilidad de su tipo de almacenamiento antes de instalar los plugins personalizados de SnapCenter.

| Máquina | Tipo de almacenamiento |
| --- | --- |
| Montajes físicos y directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM). | LUN conectados a FC |
| Y los montajes directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM). | LUN conectados a iSCSI |
| Servidores físicos y virtuales (los VMDK y LUN de RDM no son compatibles) | Volúmenes conectados en NFS |

## Privilegios mínimos de ONTAP requeridos para el plugin personalizado

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| event generate-autosupport-log |
| se muestra el historial del trabajo<br><br>detención de trabajo |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| se muestra el atributo de lun<br>lun create<br>eliminación de lun<br>geometría de lun<br>igroup de lun añadido<br>crear lun igroup<br>lun igroup eliminado<br>cambio de nombre de lun igroup<br>lun igroup show<br>asignación de lun de nodos adicionales<br>se crea la asignación de lun<br>se elimina la asignación de lun<br>asignación de lun quitar nodos de generación de informes<br>se muestra el mapa de lun<br>modificación de lun<br>movimiento de lun en volumen<br>lun desconectada<br>lun conectada<br>cambio de tamaño de lun<br>serie de lun<br>muestra de lun |
| interfaz de red |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| regla adicional de la política de snapmirror<br>regla de modificación de la política de snapmirror<br>regla de eliminación de la política de snapmirror<br>la política de snapmirror<br>restauración de snapmirror<br>de snapmirror<br>historial de snapmirror<br>actualización de snapmirror<br>conjunto de actualizaciones de snapmirror<br>destinos de listas de snapmirror |
| versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| crear el clon de volumen |
| show de clon de volumen |
| inicio de división de clon de volumen |
| detención de división de clon de volumen |
| cree el volumen |
| destrucción del volumen |
| crear el archivo de volumen |
| uso show-disk del archivo de volumen |
| volumen sin conexión |
| volumen en línea |
| modificación del volumen |
| crear el qtree de volúmenes |
| eliminación de qtree de volumen |
| modificación del qtree del volumen |
| se muestra volume qtree |
| restricción de volumen |
| visualización de volumen |
| crear snapshots de volumen |
| eliminación de snapshots de volumen |
| modificación de las copias de snapshot de volumen |
| cambio de nombre de copias de snapshot de volumen |
| restauración de copias snapshot de volumen |
| archivo de restauración de snapshots de volumen |
| visualización de copias de snapshot de volumen |
| desmonte el volumen |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| vserver cifs |
| vserver cifs share create |
| eliminación de vserver cifs share |
| se muestra vserver shadowcopy |
| visualización de vserver cifs share |
| visualización de vserver cifs |
| creación de política de exportación de vserver |
| eliminación de la política de exportación de vserver |
| creación de reglas de política de exportación de vserver |
| aparece la regla de política de exportación de vserver |
| visualización de la política de exportación de vserver |
| se muestra la conexión iscsi del vserver |
| se muestra vserver |

| Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.2.*x* y versiones posteriores |
| --- |
| interfaz de red |

## Prepare los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para los plugins personalizados

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada

sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

## Defina una estrategia de backup

Definir una estrategia de backup antes de crear las tareas de backup garantiza que se cuente con todos los backups necesarios para restaurar o clonar correctamente los recursos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

### Acerca de esta tarea

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

- Pasos*
  1. Determinar cuándo se debe realizar el backup de los recursos.
  2. Decidir cuántas tareas de backup se necesitan.
  3. Decidir el nombre que se asignará a los backups.
  4. Decidir si se harán copias de Snapshot de los grupos de consistencia y elegir las opciones apropiadas para eliminar las copias.
  5. Decidir si se desean usar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
  6. Determinar el período de retención para las copias de Snapshot en el sistema de almacenamiento de origen y el destino de SnapMirror.
  7. Determinar si se desea ejecutar comandos antes o después de la operación de backup y proporcionar un script previo o posterior.

## Estrategia de backup para plugins personalizados

### Programaciones de backup de recursos de plugins personalizados

El factor más importante para determinar una programación de backup es la tasa de cambio del recurso. Mientras más frecuentes sean los backups de los recursos, menos archivos de registro necesitará SnapCenter para la restauración, lo cual puede acelerar las operaciones de restauración.

Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores que se deben tener en cuenta son la importancia del recurso para la organización, el SLA y el RPO.

El SLA define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y RPO ayudan a establecer una estrategia de protección de datos.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de backup (cada cuánto se deben realizar los backups), también denominada tipo de programación para algunos plugins, es parte de una configuración de políticas. Por ejemplo, se puede configurar una frecuencia de backup horaria, diaria, semanal o mensual. Puede acceder a las directivas en la interfaz gráfica de usuario de SnapCenter haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

  Las programaciones de backup (el momento exacto en que se realiza el backup) forman parte de la configuración de un recurso o un grupo de recursos. Por ejemplo, si hay un grupo de recursos con una política configurada para realizar un backup semanal, es posible configurar la programación para que se realice un backup todos los jueves a las 00:10 Para acceder a las programaciones de grupos de recursos en la interfaz gráfica de usuario de SnapCenter, haga clic en **Recursos**, seleccione el complemento adecuado y haga clic en **Ver** > **Grupo de recursos**.

#### Cantidad de trabajos de backup necesarios

Algunos factores que determinan la cantidad de trabajos de backup que se necesitan son el tamaño del recurso, la cantidad de volúmenes que se usan, la tasa de cambio del recurso y el acuerdo de nivel de servicio.

La cantidad de trabajos de backup que se selecciona depende de la cantidad de volúmenes en los que se colocaron los recursos. Por ejemplo, si se colocó un grupo de recursos pequeños en un volumen y un recurso grande en otro volumen, puede ser necesario crear un trabajo de backup para los recursos pequeños y otro trabajo para el recurso grande.

## Tipos de estrategias de restauración compatibles con los recursos de SAP HANA añadidos manualmente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter. Existen dos tipos de estrategias de restauración para los recursos de SAP HANA que se añaden manualmente. No puede recuperar los recursos de SAP HANA añadidos manualmente.

No puede recuperar los recursos de SAP HANA añadidos manualmente.

#### Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

#### Restauración de nivel de archivos

- Restaura los archivos de volúmenes, qtrees o directorios

- Restaura solo los LUN seleccionados

# Desarrolle un complemento para la aplicación

## Descripción general

El servidor de SnapCenter permite poner en marcha y gestionar sus aplicaciones como complementos en SnapCenter. Las aplicaciones de su elección pueden conectarse al servidor de SnapCenter para disfrutar de funcionalidades de protección y gestión de datos.

SnapCenter le permite desarrollar complementos personalizados utilizando diferentes lenguajes de programación. Puede desarrollar un complemento personalizado utilizando Perl, Java, BATCH u otros lenguajes de scripting.

Para utilizar plugins personalizados en SnapCenter, debe realizar las siguientes tareas:

- Cree un complemento para su aplicación siguiendo las instrucciones de esta guía
- Cree un archivo de descripción
- Exporte el plugin personalizado para instalarlo en el host de SnapCenter
- Cargue el archivo zip del plugin en el servidor de SnapCenter

#### Gestión de complementos genérica en todas las llamadas API

Para cada llamada a la API, utilice la siguiente información:

- Parámetros del plugin
- códigos de salida
- Registrar mensajes de error
- Coherencia de datos

##### Utilice los parámetros del plugin

Se pasa un conjunto de parámetros al plug-in como parte de cada llamada API realizada. En la siguiente tabla, se muestra información específica de los parámetros.

| Parámetro | Específico |
|---|---|
| ACCIÓN | Determina el nombre del flujo de trabajo. Por ejemplo, descubra, copia de seguridad, archivoOrVolRestore o cloneVolAndLun |
| RECURSOS | Enumera los recursos que se deben proteger. UID y tipo identifican un recurso. La lista se presenta al plugin con el siguiente formato:<br><br>“<UID>,<TYPE>;<UID>,<TYPE>”. Por ejemplo, “Instance1,instancia;Instance2\\DB1,base de datos” |

| Parámetro | Específico |
| --- | --- |
| NOMBRE_APLICACIÓN | Determina qué plugin se está utilizando. Por ejemplo, DB2, MYSQL. El servidor SnapCenter cuenta con compatibilidad integrada para las aplicaciones de la lista. Este parámetro distingue mayúsculas de minúsculas. |
| APP_IGNORE_ERROR | (Y o N) esto hace que SnapCenter salga o no salga cuando se encuentra un error de aplicación. Esto es útil cuando se realiza el backup de varias bases de datos y no se desea que un solo fallo detenga la operación de backup. |
| <RESOURCE_NAME>__APP_INSTANCE_USERNAME | Se han establecido las credenciales de SnapCenter para el recurso. |
| <RESOURCE_NAME>_APP_INSTANCE_PASSWORD | Se han establecido las credenciales de SnapCenter para el recurso. |
| <CUSTOM_PARAM>_<RESOURCE_NAME> | Todos los valores de clave personalizada de nivel de recursos están disponibles para los plug-ins con “<RESOURCE_NAME>_”. Por ejemplo, si una clave personalizada es “MASTER_SLAVE” para un recurso llamado “MySQLDB”, estará disponible como MySQLDB_MASTER_SLAVE |

#### Utilice los códigos de salida

El plugin devuelve el estado de la operación a su host mediante códigos de salida. Cada código tiene un significado específico y el plug-in utiliza el código de salida derecho para indicar lo mismo.

En la siguiente tabla se muestran los códigos de error y su significado.

| Código de salida | Específico |
| --- | --- |
| 0 | Funcionamiento correcto. |
| 99 | La operación solicitada no es compatible o está implementada. |
| 100 | Error en la operación, omita la pausa y salga. La función de inactividad está predeterminada. |
| 101 | Error en la operación, continúe con la operación de backup. |
| otros | Error en la operación, ejecución de la reanudación y salida. |

#### Registrar mensajes de error

Los mensajes de error pasan del plugin al servidor de SnapCenter. El mensaje incluye el mensaje, el nivel de registro y la Marca de hora.

En la tabla siguiente se enumeran los niveles y sus propósitos.

| Parámetro | Específico |
|---|---|
| INFORMACIÓN | mensaje informativo |
| ADVERTIR | mensaje de advertencia |
| ERROR | mensaje de error |
| DEPURAR | depurar mensaje |
| TRAZA | mensaje de seguimiento |

#### Conserve la consistencia de datos

Los plugins personalizados conservan datos entre operaciones de la misma ejecución del flujo de trabajo. Por ejemplo, un plugin puede almacenar datos al final de la inactividad, que se puede utilizar durante la operación de inactivación.

Los datos que se van a conservar se establecen como parte del objeto de resultado mediante el complemento. Sigue un formato específico y se describe con detalle en cada estilo de desarrollo de complementos.

## Desarrollo basado en PERL

Debe seguir ciertas convenciones mientras desarrolla el plugin con PERL.

- El contenido debe ser legible
- Debe implementar la configuración de operaciones obligatorias, el modo de inactividad y la reanudación
- Debe utilizar una sintaxis específica para devolver los resultados al agente
- El contenido debe guardarse como archivo <PLUGIN_NAME>.pm

Las operaciones disponibles son

- Setenv
- versión
- modo de inactividad
- inactivación
- clone_pre, clone_post
- restaurar_pre, restaurar
- limpieza

## Manejo general del plug-in

### Uso del objeto Results

Todas las operaciones de plugin personalizado deben definir el objeto Results. Este objeto envía mensajes, código de salida, stdout y stderr de vuelta al agente host.

Objeto resultados:

```
my $result = {
```

```
      exit_code => 0,
      stdout => "",
      stderr => "",
};
```

Devolver el objeto Results:

```
return $result;
```

### Conservación de la coherencia de los datos

Es posible conservar datos entre operaciones (excepto limpieza) como parte de la misma ejecución del flujo de trabajo. Esto se logra usando pares clave-valor. Los pares clave-valor de los datos se establecen como parte del objeto de resultado y se conservan y están disponibles en las operaciones posteriores del mismo flujo de trabajo.

En el ejemplo de código siguiente se establecen los datos que se van a conservar:

```
my $result = {
  exit_code => 0,
  stdout => "",
  stderr => "",
};
  $result->{env}->{'key1'} = 'value1';
  $result->{env}->{'key2'} = 'value2';
  ….
  return $result
```

El código anterior establece dos pares clave-valor, que están disponibles como entrada en la operación posterior. Los dos pares clave-valor se pueden acceder mediante el siguiente código:

```
sub setENV {
    my ($self, $config) = @_;
    my $first_value = $config->{'key1'};
    my $second_value = $config->{'key2'};
    …
}
```

```
 === Logging error messages
Cada operación puede enviar mensajes al agente host, que muestra y
almacena el contenido. Un mensaje contiene el nivel de mensaje, una Marca
de tiempo y un texto de mensaje. Se admiten mensajes multilínea.
```

```
Load the SnapCreator::Event Class:
my $msgObj = new SnapCreator::Event();
my @message_a = ();
```

Utilice el método msgObj para capturar un mensaje mediante el método Collect.

```
$msgObj->collect(\@message_a, INFO, "My INFO Message");
$msgObj->collect(\@message_a, WARN, "My WARN Message");
$msgObj->collect(\@message_a, ERROR, "My ERROR Message");
$msgObj->collect(\@message_a, DEBUG, "My DEBUG Message");
$msgObj->collect(\@message_a, TRACE, "My TRACE Message");
```

Aplicar mensajes al objeto resultados:

```
$result->{message} = \@message_a;
```

#### Uso de los espárragos del plug-in

Los plugins personalizados deben exponer los talones del plug-in. Estos son métodos a los que llama el servidor SnapCenter, en función de un flujo de trabajo.

| Muñón de complemento | Opcional/obligatorio | Específico |
| --- | --- | --- |
| Setenv | obligatorio | Este código auxiliar establece el entorno y el objeto de configuración.<br><br>Aquí se debe realizar cualquier análisis o manejo del entorno. Cada vez que se llama un archivo stub, el archivo stub setenv se llama justo antes. Solo es necesario para complementos DE tipo PERL. |
| Versión | Opcional | Este código auxiliar se utiliza para obtener la versión de la aplicación. |
| Detección | Opcional | Este archivo stub se utiliza para detectar objetos de aplicación como la instancia o la base de datos alojada en el agente o host.<br><br>Se espera que el complemento devuelva los objetos de aplicación detectados en un formato específico como parte de la respuesta. Este código auxiliar sólo se utiliza en caso de que la aplicación esté integrada con SnapDrive para Unix.<br><br> Sistema de archivos Linux (Linux Flavors) es compatible. AIX/Solaris (Unix Flavors) no son compatibles. |

| Muñón de complemento | Opcional/obligatorio | Específico |
| --- | --- | --- |
| discovery_complete | Opcional | Este archivo stub se utiliza para detectar objetos de aplicación como la instancia o la base de datos alojada en el agente o host.<br><br>Se espera que el complemento devuelva los objetos de aplicación detectados en un formato específico como parte de la respuesta. Este código auxiliar sólo se utiliza en caso de que la aplicación esté integrada con SnapDrive para Unix.<br><br>Sistema de archivos Linux (Linux Flavors) es compatible. AIX y Solaris (versiones Unix) no son compatibles. |
| Modo de inactividad | obligatorio | Este archivo stub es responsable de realizar un modo de inactividad, lo que significa colocar la aplicación en un estado en el que puede crear una copia Snapshot. Esto se llama antes de la operación de copia de Snapshot. Los metadatos de la aplicación que se conservará deben definirse como parte de la respuesta, que se devolverá durante las operaciones posteriores de clonado o restauración en la copia Snapshot de almacenamiento correspondiente en forma de parámetros de configuración. |
| Inactivación | obligatorio | Este código auxiliar es responsable de realizar un modo de inactividad, lo que significa poner la aplicación en un estado normal. Esto se llama después de crear una copia Snapshot. |

| Muñón de complemento | Opcional/obligatorio | Específico |
| --- | --- | --- |
| clone_pre | opcional | Este archivo stub es responsable de realizar tareas previas a la clonación. Se supone que se utiliza la interfaz de clonación del servidor de SnapCenter integrada y se activa al realizar la operación de clonación. |
| clone_post | opcional | Este archivo stub es responsable de realizar tareas posteriores a la clonación. Esto supone que se utiliza la interfaz de clonación del servidor de SnapCenter integrada y se activa solo al realizar una operación de clonado. |
| restaurar_pre | opcional | Este archivo stub es responsable de realizar tareas prerestore. Esto supone que se utiliza la interfaz de restauración de servidor de SnapCenter incorporada y se activa al realizar una operación de restauración. |
| Restaurar | opcional | Este código auxiliar es responsable de realizar tareas de restauración de aplicaciones. Esto supone que se utiliza la interfaz de restauración de servidor de SnapCenter incorporada y que solo se activa al realizar una operación de restauración. |

| Muñón de complemento | Opcional/obligatorio | Específico |
| --- | --- | --- |
| Limpieza | opcional | Este archivo stub es responsable de realizar una limpieza después de las operaciones de backup, restauración o clonado. La limpieza puede realizarse durante la ejecución normal del flujo de trabajo o en caso de que se produzca un error en el mismo. Puede inferir el nombre del flujo de trabajo bajo el cual se llama a la limpieza haciendo referencia a LA ACCIÓN de parámetro de configuración, que puede ser copia de seguridad, clonVolAndLun o archivoOrVolRestore. El parámetro DE configuración ERROR_MESSAGE indica si se produjo algún error al ejecutar el flujo de trabajo. Si ERROR_MESSAGE está definido y NO es NULL, se llama a la limpieza durante la ejecución de un fallo de flujo de trabajo. |
| versión_aplicación | Opcional | SnapCenter utiliza este archivo stub para que el complemento gestione el detalle de la versión de la aplicación. |

#### Información sobre el paquete de plugins

Cada plugin debe tener la siguiente información:

```
package MOCK;
our @ISA = qw(SnapCreator::Mod);
=head1 NAME
MOCK - class which represents a MOCK module.
=cut
=head1 DESCRIPTION
MOCK implements methods which only log requests.
=cut
use strict;
use warnings;
use diagnostics;
use SnapCreator::Util::Generic qw ( trim isEmpty );
use SnapCreator::Util::OS qw ( isWindows isUnix getUid
createTmpFile );
use SnapCreator::Event qw ( INFO ERROR WARN DEBUG COMMENT ASUP
CMD DUMP );
my $msgObj = new SnapCreator::Event();
my %config_h = ();
```

#### Operaciones

Puede codificar varias operaciones, como setenv, Version, Quiesce y UnQUIESCE, que son compatibles con los plug-ins personalizados.

### Funcionamiento de setenv

La operación setenv es necesaria para los complementos creados con PERL. Puede ajustar el ENV y acceder fácilmente a los parámetros del plug-in.

```
sub setENV {
    my ($self, $obj) = @_;
    %config_h = %{$obj};
    my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
    };
    return $result;
}
```

### Operación de versión

La operación de versión devuelve la información de la versión de la aplicación.

```
sub version {
  my $version_result = {
    major => 1,
    minor => 2,
    patch => 1,
    build => 0
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $version_result->{message} = \@message_a;
  return $version_result;
}
```

**Operaciones de inactivación**

La operación de inactividad realiza una operación de inactividad de la aplicación en los recursos que se enumeran en el parámetro RESOURCES.

```
sub quiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

**Funcionamiento de la reanudación**

La operación de inactividad es necesaria para desactivar la activación de la aplicación. La lista de recursos está disponible en el parámetro RESOURCES.

```
sub unquiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::unquiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

## Estilo NATIVO

SnapCenter admite lenguajes que no SEAN DE programación PERL o lenguajes de scripting para crear complementos. Esto se conoce como programación DE estilo NATIVO, que puede ser un archivo de secuencia de comandos o LOTE.

Los plugins DE estilo NATIVO deben seguir ciertas convenciones indicadas a continuación:

El plugin debe ser ejecutable

- Para los sistemas Unix, el usuario que ejecuta el agente debe tener privilegios de ejecución en el plug-in
- En los sistemas Windows, los complementos de PowerShell deben tener el sufijo .ps1, los demás scripts de Windows deben tener el sufijo .cmd o .bat y el usuario debe ser ejecutable
- Los complementos deben reaccionar a los argumentos de la línea de comandos, como "-QUIESCE", "-unQUIESCE"
- Los plug-ins deben devolver código de salida 99 en caso de que no se haya implementado una operación o función
- Los plugins deben utilizar una sintaxis específica para devolver los resultados al servidor

### Manejo general del plug-in

#### Mensajes de error de registro

Cada operación puede enviar mensajes al servidor, que muestra y almacena el contenido. Un mensaje contiene el nivel de mensaje, una Marca de tiempo y un texto de mensaje. Se admiten mensajes multilínea.

Formato:

```
SC_MSG#<level>#<timestamp>#<message>
SC_MESSAGE#<level>#<timestamp>#<message>
```

#### Uso de los espárragos del plug-in

Los complementos de SnapCenter deben implementar espárragos de complemento. Estos son métodos a los que el servidor SnapCenter llama en función de un flujo de trabajo específico.

| Muñón de complemento | Opcional/obligatorio | Específico |
|---|---|---|
| modo de inactividad | obligatorio | Este código auxiliar es responsable de realizar una pausa. Coloca la aplicación en un estado en el que podemos crear una copia Snapshot. Esto se denomina antes de la operación de copia de Snapshot de almacenamiento. |
| inactivación | obligatorio | Este código auxiliar es responsable de realizar una pausa. Coloca la aplicación en un estado normal. Esto se denomina después de la operación de copia de Snapshot de almacenamiento. |
| clone_pre | opcional | Este archivo stub es responsable de realizar tareas previas a la clonación. Esto supone que se utiliza la interfaz de clonado de SnapCenter incorporada y que solo se activa mientras se realiza la acción "clone_vol o clone_lun". |
| clone_post | Opcional | Este archivo stub es responsable de realizar tareas posteriores a la clonación. Esto supone que utiliza la interfaz de clonado de SnapCenter integrada y que solo se activa mientras se realizan operaciones de «clone_vol o clone_lun». |
| restaurar_pre | Opcional | Este archivo stub es responsable de realizar tareas previas a la restauración. Esto supone que se utiliza la interfaz de restauración de SnapCenter integrada y que solo se activa durante la operación de restauración. |

| Muñón de complemento | Opcional/obligatorio | Específico |
| --- | --- | --- |
| restaurar | opcional | Este código auxiliar es responsable de realizar todas las acciones de restauración. Esto supone que no está utilizando la interfaz de restauración integrada. Se activa durante la operación de restauración. |

#### Ejemplos

### Windows PowerShell

Compruebe si la secuencia de comandos se puede ejecutar en el sistema. Si no puede ejecutar la secuencia de comandos, defina el desvío de Set-ExecutionPolicy para la secuencia de comandos y vuelva a intentar la operación.

```
if ($args.length -ne 1) {
  write-warning "You must specify a method";
  break;
}
function log ($level, $message) {
  $d = get-date
  echo "SC_MSG#$level#$d#$message"
}
function quiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Quiescing application using script $app_name";
  log "INFO" "Quiescing application finished successfully"
}
function unquiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Unquiescing application using script $app_name";
  log "INFO" "Unquiescing application finished successfully"
}
  switch ($args[0]) {
    "-quiesce" {
    quiesce;
}
"-unquiesce" {
    unquiesce;
}
default {
    write-error "Function $args[0] is not implemented";
    exit 99;
  }
}
exit 0;
```

## Estilo Java

Un complemento personalizado de Java interactúa directamente con una aplicación como base de datos, instancia, etc.

#### Limitaciones

Existen ciertas limitaciones que debe tener en cuenta al desarrollar un plug-in utilizando el lenguaje de programación Java.

| Característica de plug-in | Plugin de Java |
| --- | --- |
| Complejidad | De bajo a mediano |

| Característica de plug-in | Plugin de Java |
| --- | --- |
| Huella de la memoria | Hasta 10-20 MB |
| Dependencias con otras bibliotecas | Bibliotecas para la comunicación de aplicaciones |
| Número de subprocesos | 1 |
| Tiempo de ejecución de subprocesos | Menos de una hora |

#### Motivo de las limitaciones de Java

El objetivo del agente SnapCenter es garantizar una integración de aplicaciones sólida, segura y continua. Al admitir plug-ins de Java, es posible que los plug-ins introduzcan fugas de memoria y otros problemas no deseados. Esas cuestiones son difíciles de abordar, especialmente cuando el objetivo es mantener las cosas fáciles de usar. Si la complejidad de un complemento no es demasiado compleja, es mucho menos probable que los desarrolladores hubieran introducido los errores. El peligro del plug-in Java es que se ejecuten en la misma JVM que el propio agente de SnapCenter. Cuando el plug-in se bloquea o pierde memoria, también puede afectar negativamente al agente.

### Métodos admitidos

| Método | Obligatorio | Descripción | ¿Cuándo y por quién? |
| --- | --- | --- | --- |
| Versión | Sí | Necesita obtener la versión del plugin. | El servidor o el agente de SnapCenter para solicitar la versión del plugin. |
| Modo de inactividad | Sí | Necesita realizar una pausa en la aplicación. En la mayoría de los casos, esto implica poner la aplicación en un estado donde SnapCenter Server puede crear un backup (por ejemplo, una copia Snapshot). | Antes de que el servidor de SnapCenter cree una copia de Snapshot o realice un backup en general. |
| Inactivación | Sí | Necesita realizar una reanudación de la aplicación. En la mayoría de los casos, esto significa volver a poner la aplicación en un estado de funcionamiento normal. | Después de que el servidor SnapCenter haya creado una copia de Snapshot o haya realizado un backup en general. |

| Método | Obligatorio | Descripción | ¿Cuándo y por quién? |
|---|---|---|---|
| Limpieza | No | Responsable de la limpieza de cualquier cosa que el plug-in necesite limpiar. | Cuando termina un flujo de trabajo en el servidor SnapCenter (correctamente o con un error). |
| ClonPree | No | Debe realizar las acciones que deben realizarse antes de realizar una operación de clonado. | Cuando un usuario activa una acción "clonVol" o "clonLun" y utiliza el asistente de clonación integrado (GUI/CLI). |
| ClonPost | No | Debe realizar las acciones que deben realizarse después de realizar una operación de clonado. | Cuando un usuario activa una acción "clonVol" o "clonLun" y utiliza el asistente de clonación integrado (GUI/CLI). |
| RestauradoPre | No | Debe ejecutar acciones que deben realizarse antes de solicitar la operación de restauración. | Cuando un usuario activa una operación de restauración. |
| Restaurar | No | Responsable de la restauración/recuperación de una aplicación. | Cuando un usuario activa una operación de restauración. |
| Versión de appVersion | No | Para recuperar la versión de la aplicación que gestiona el plugin. | Como parte de la recogida de datos de ASUP en cada flujo de trabajo, como Backup/Restore/Clone. |

### Tutorial

En esta sección se describe cómo crear un complemento personalizado mediante el lenguaje de programación Java.

#### Configuración de eclipse

1. Cree un nuevo proyecto Java "TutorialPlugin" en Eclipse
2. Haga clic en **Finalizar**
3. Haga clic con el botón derecho del ratón en **nuevo proyecto → Propiedades → Java Build Path → Bibliotecas → Añadir tarros externos**
4. Desplácese a la carpeta ../lib/ del agente anfitrión y seleccione Jarras scAgent-5.0-core.jar y common-5.0.jar

5. Seleccione el proyecto y haga clic con el botón derecho del ratón en la carpeta **src → Nuevo → paquete** y cree un nuevo paquete con el nombre com.netapp.snapcreator.agent.plugin.TutorialPlugin
6. Haga clic con el botón derecho del ratón en el nuevo paquete y seleccione Nuevo → clase Java.
   a. Introduzca el nombre como TutorialPlugin.
   b. Haga clic en el botón de exploración de la superclase y busque "*AbstractPlugin". Sólo debe aparecer un resultado:

```
 "AbstractPlugin - com.netapp.snapcreator.agent.nextgen.plugin".
.. Haga clic en *Finalizar*.
.. Clase Java:
```

```
package com.netapp.snapcreator.agent.plugin.TutorialPlugin;
import
com.netapp.snapcreator.agent.nextgen.common.result.Describe
Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.VersionR
esult;
import
com.netapp.snapcreator.agent.nextgen.context.Context;
import
com.netapp.snapcreator.agent.nextgen.plugin.AbstractPlugin;
public class TutorialPlugin extends AbstractPlugin {
  @Override
  public DescribeResult describe(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result quiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result unquiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public VersionResult version() {
    // TODO Auto-generated method stub
    return null;
  }
}
```

#### Implementación de los métodos necesarios

La función de inactividad, la reanudación y la versión son métodos obligatorios que cada plugin de Java personalizado debe implementar.

A continuación, se muestra un método de versión para obtener la versión del plugin.

```
@Override
public VersionResult version() {
    VersionResult versionResult = VersionResult.builder()
                                                .withMajor(1)
                                                .withMinor(0)
                                                .withPatch(0)
                                                .withBuild(0)
                                                .build();
    return versionResult;
}
```

```
Below is the implementation of quiesce and unquiesce method. These will be
interacting with   the application, which is being protected by SnapCenter
Server. As this is just a tutorial, the
application part is not explained, and the focus is more on the
functionality that SnapCenter   Agent provides the following to the plug-
in developers:
```

```
@Override
  public Result quiesce(Context context) {
    final Logger logger = context.getLogger();
    /*
      * TODO: Add application interaction here
    */
```

```
logger.error("Something bad happened.");
logger.info("Successfully handled application");
```

```
    Result result = Result.builder()
                    .withExitCode(0)
                    .withMessages(logger.getMessages())
                    .build();
    return result;
}
```

El método se pasa en un objeto de contexto. Contiene varios asistentes, por ejemplo, un registrador y un almacén de contexto, así como información sobre la operación actual (Workflow-ID, Job-ID). Podemos obtener el registrador llamando al registrador de registros final = context.getLogger();. El objeto logger proporciona métodos similares conocidos por otros marcos de registro, por ejemplo, logback. En el objeto Result, también puede especificar el código de salida. En este ejemplo, se devuelve cero, ya que no hubo ningún problema. Otros códigos de salida pueden asignar a diferentes situaciones de fallo.

#### Utilizando el objeto Resultado

El objeto Result contiene los parámetros siguientes:

| Parámetro | Predeterminado | Descripción |
|---|---|---|
| Gestión de | Configuración vacía | Este parámetro se puede utilizar para enviar parámetros de configuración al servidor. Puede ser parámetros que el plugin desea actualizar. Si este cambio se refleja realmente en la configuración del servidor SnapCenter depende del parámetro APP_CONF_PERSISTENCY=y o N de la configuración. |
| ExitCode | 0 | Indica el estado de la operación. Un "0" significa que la operación se ejecutó correctamente. Otros valores indican errores o advertencias. |
| Apedrear | Lista vacía | Esto se puede utilizar para transmitir mensajes stdout al servidor SnapCenter. |
| Stderr | Lista vacía | Esto se puede utilizar para transmitir mensajes stderr de nuevo al servidor SnapCenter. |
| Mensajes | Lista vacía | Esta lista contiene todos los mensajes que un plug-in desea volver al servidor. El servidor SnapCenter muestra esos mensajes en la CLI o en la GUI. |

El agente de SnapCenter proporciona constructores ("Patrón de creación") para todos sus tipos de resultados. Esto hace que su uso sea muy sencillo:

```
Result result = Result.builder()
                    .withExitCode(0)
                    .withStdout(stdout)
                    .withStderr(stderr)
                    .withConfig(config)
                    .withMessages(logger.getMessages())
                    .build()
```

Por ejemplo, establezca el código de salida en 0, establezca las listas para stdout y stderr, defina los parámetros de configuración y también agregue los mensajes de registro que se enviarán de nuevo al

servidor. Si no necesita todos los parámetros, envíe sólo los que necesite. Como cada parámetro tiene un valor predeterminado, si quita .witEExitCode(0) del código siguiente, el resultado no se verá afectado:

```
Result result = Result.builder()
                      .withExitCode(0)
                      .withMessages(logger.getMessages())
                      .build();
```

#### VersionResult

VersionResult informa a SnapCenter Server de la versión del plugin. Como también hereda del resultado, contiene los parámetros config, exitCode, stdout, stderr y messages.

| Parámetro | Predeterminado | Descripción |
|---|---|---|
| Importante | 0 | Campo de versión principal del plugin. |
| Menor | 0 | Campo de versión secundaria del plugin. |
| Parche | 0 | Campo de versión de revisión del plugin. |
| Cree | 0 | Cree el campo de versión del plugin. |

Por ejemplo:

```
VersionResult result = VersionResult.builder()
                                    .withMajor(1)
                                    .withMinor(0)
                                    .withPatch(0)
                                    .withBuild(0)
                                    .build();
```

#### Uso del objeto de contexto

El objeto Context proporciona los siguientes métodos:

| Método de contexto | Específico |
|---|---|
| String getWorkflowId(); | Devuelve el ID de flujo de trabajo que utiliza el servidor SnapCenter para el flujo de trabajo actual. |

| Método de contexto | Específico |
| --- | --- |
| Config getconfig(); | Devuelve la configuración que se envía desde el servidor SnapCenter al agente. |

#### ID del flujo de trabajo

El ID de flujo de trabajo es el ID que utiliza el servidor de SnapCenter para hacer referencia a un flujo de trabajo en ejecución específico.

#### Gestión de

Este objeto contiene (la mayoría) los parámetros que un usuario puede establecer en la configuración del servidor SnapCenter. Sin embargo, debido a razones de seguridad, algunos de esos parámetros pueden filtrarse en el servidor. A continuación figura un ejemplo de cómo acceder a la configuración y recuperar un parámetro:

```
final Config config = context.getConfig();
String myParameter =
config.getParameter("PLUGIN_MANDATORY_PARAMETER");
```

""// MyParameter" contiene ahora el parámetro leído en la configuración del servidor SnapCenter Si no existe una clave de parámetro config, devolverá un valor de tipo String vacío ("").

#### Exportando el plugin

Debe exportar el plugin para instalarlo en el host de SnapCenter.

En Eclipse, realice las siguientes tareas:

1. Haga clic con el botón derecho en el paquete básico del complemento (en nuestro ejemplo com.netapp.snapcreator.agent.plugin.TutorialPlugin).
2. Seleccione **Exportar → Java → Archivo Jar**
3. Haga clic en **Siguiente**.
4. En la siguiente ventana, especifique la ruta de acceso de archivo JAR de destino: tutorial_plugin.jar la clase base del plugin se denomina TutorialPlugin.class, el plug-in debe agregarse a una carpeta con el mismo nombre.

Si el plugin depende de bibliotecas adicionales, puede crear la siguiente carpeta: Lib/

Puede agregar archivos JAR en los que depende el plugin (por ejemplo, un controlador de base de datos). Cuando SnapCenter carga el plug-in, asocia automáticamente todos los archivos JAR de esta carpeta y los añade a la classpath.

## Plugin personalizado en SnapCenter

### Plugin personalizado en SnapCenter

El complemento personalizado creado con Java, PERL o estilo NATIVO puede instalarse en el host utilizando SnapCenter Server para permitir la protección de datos de su aplicación. Debe haber exportado el plugin para

instalarlo en el host SnapCenter mediante el procedimiento proporcionado en este tutorial.

#### Crear un archivo de descripción del plugin

Para cada plugin creado, debe tener un archivo de descripción. El archivo de descripción describe los detalles del plugin. El nombre del archivo debe ser Plugin_descriptor.xml.

### Usar atributos del archivo descriptor del plugin y su importancia

| Atributo | Descripción |
|---|---|
| Nombre | Nombre del plugin. Se permiten caracteres alfanuméricos. Por ejemplo, DB2, MYSQL, MongoDB<br><br>Para los plugins creados con un estilo NATIVO, asegúrese de no proporcionar la extensión del archivo. Por ejemplo, si el nombre del plugin es MongoDB.sh, especifique el nombre como MongoDB. |
| Versión | Versión de plugin. Puede incluir tanto la versión principal como la secundaria. Por ejemplo, 1.0, 1.1, 2.0, 2.1 |
| DisplayName | El nombre del plugin que se mostrará en SnapCenter Server. Si se escriben varias versiones del mismo complemento, asegúrese de que el nombre para mostrar es el mismo en todas las versiones. |
| PluginType | Idioma utilizado para crear el plug-in. Los valores admitidos son Perl, Java y Native. El tipo de complemento nativo incluye scripts de shell de Unix/Linux, scripts de Windows, Python o cualquier otro lenguaje de scripting. |
| OSNAME | El nombre del sistema operativo del host donde se ha instalado el plugin. Los valores válidos son Windows y Linux. Es posible que un único complemento esté disponible para su puesta en marcha en varios tipos de sistemas operativos, como el complemento DE tipo PERL. |
| OSVersion | La versión del sistema operativo del host donde se instaló el plugin. |
| ResourceName | Nombre del tipo de recurso que admite el plugin. Por ejemplo, base de datos, instancia, colecciones. |

| Atributo | Descripción |
| --- | --- |
| Padre | En caso de que el ResourceName dependa jerárquicamente de otro tipo de recurso y, a continuación, Parent determina el atributo resourcetype primario.<br><br>Por ejemplo, el complemento DB2, ResourceName “Database” tiene una “instancia” principal. |
| RequireFileSystemPlugin | Sí o no Determina si la pestaña Recovery se muestra en el asistente Restore. |
| ResourceRequiresAuthentication | Sí o no Determina si los recursos, que se detectan automáticamente o no se detectan automáticamente necesitan credenciales para realizar las operaciones de protección de datos después de detectar el almacenamiento. |
| RequireFileSystemClone | Sí o no Determina si el plugin requiere la integración del plugin del sistema de archivos para el flujo de trabajo de clonado. |

A continuación, se muestra un ejemplo del archivo Plugin_descriptor.xml para el plugin personalizado DB2:

```
<Plugin>
<SMSServer></SMSServer>
<Name>DB2</Name>
<Version>1.0</Version>
<PluginType>Perl</PluginType>
<DisplayName>Custom DB2 Plugin</DisplayName>
<SupportedOS>
<OS>
<OSName>windows</OSName>
<OSVersion>2012</OSVersion>
</OS>
<OS>
<OSName>Linux</OSName>
<OSVersion>7</OSVersion>
</OS>
</SupportedOS>
<ResourceTypes>
<ResourceType>
<ResourceName>Database</ResourceName>
<Parent>Instance</Parent>
</ResourceType>
<ResourceType>
<ResourceName>Instance</ResourceName>
</ResourceType>
</ResourceTypes>
<RequireFileSystemPlugin>no</RequireFileSystemPlugin>
<ResourceRequiresAuthentication>yes</ResourceRequiresAuthentication>
<SupportsApplicationRecovery>yes</SupportsApplicationRecovery>
</Plugin>
```

#### Creación de un archivo ZIP

Después de desarrollar un plugin y crear un archivo descriptor, es necesario añadir los archivos del plugin y el archivo Plugin_descriptor.xml a una carpeta y zip.

Debe tener en cuenta lo siguiente antes de crear un archivo ZIP:

- El nombre de script debe ser el mismo que el del plugin.
- Para el plugin PERL, la carpeta ZIP debe contener una carpeta con el archivo de script y el archivo descriptor debe estar fuera de esta carpeta. El nombre de la carpeta debe ser el mismo que el del plugin.
- Para los plugins distintos al plugin PERL, la carpeta ZIP debe contener el descriptor y los archivos de script.
- La versión de SO debe ser un número.

Ejemplos:

- DB2 plug-in: Agregue el archivo DB2.pm y Plugin_descriptor.xml a “DB2.zip”.
- Plug-in desarrollado con Java: Añada archivos JAR, archivos JAR dependientes y archivo Plugin_descriptor.xml a una carpeta y zip.

#### Cargando el archivo ZIP del plugin

Es necesario cargar el archivo ZIP del plugin en el servidor de SnapCenter para que el plugin se pueda implementar en el host deseado.

Puede cargar el plugin mediante la interfaz de usuario o cmdlets de.

**UI:**

- Cargue el archivo ZIP del plug-in como parte del asistente de flujo de trabajo **Add** o **Modify Host**
- Haga clic en **“Seleccionar para cargar el complemento personalizado”**

**PowerShell:**

- Cmdlet Upload-SmPluginPackage

  Por ejemplo, PS> Upload-SmPluginPackage -AbsolutePath c:\DB2_1.zip

  Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte la información de referencia sobre cmdlets.

"Guía de referencia de cmdlets de SnapCenter Software".

#### Implementación de los plugins personalizados

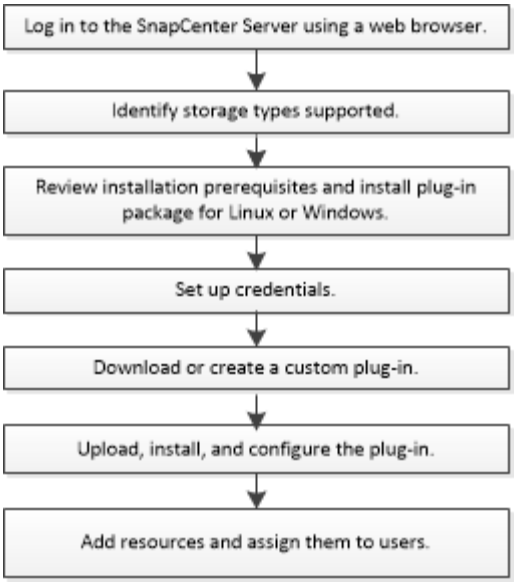
El complemento personalizado cargado ahora está disponible para su implementación en el host deseado como parte del flujo de trabajo **Add** y **Modify Host**. Es posible cargar varias versiones de plugins en SnapCenter Server y seleccionar la versión deseada para implementarla en un host específico.

Para obtener más información sobre cómo cargar el plugin, consulte, "Añada hosts e instale paquetes de plugins en hosts remotos"

# Prepare la instalación de los plugins personalizados de SnapCenter

## Flujo de trabajo de instalación de plugins personalizados de SnapCenter

Deber instalar y configurar plugins personalizados de SnapCenter si desea proteger los recursos de plugins personalizados.




"Desarrolle un complemento para la aplicación"

## Requisitos previos para añadir hosts e instalar plugins personalizados de SnapCenter

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos. Los plugins personalizados se pueden utilizar tanto en entornos de Windows como de Linux.

- Debe haber creado un plugin personalizado. Para obtener detalles, consulte la información para el desarrollador.

  "Desarrolle un complemento para la aplicación"

- Si desea gestionar aplicaciones MySQL o DB2, debe haber descargado los plugins personalizados MySQL y DB2 que suministra NetApp.
- Debe haber instalado la versión de 64 bit de Java 1.8 en su host Linux o de Windows.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Los plugins personalizados deben estar disponibles en el host del cliente desde el que se ejecuta la operación de añadir host.

### Generales

Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.

### Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Si gestiona nodos de clúster en SnapCenter, debe tener un usuario con privilegios de administrador para todos los nodos del clúster.

**Hosts Linux**

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java de 1.8 64 bits en el host Linux.

  Si utiliza Windows 2019 o Windows 2016 para el host de SnapCenter Server, debe instalar Java 1.8 de 64 bits. La herramienta de matriz de interoperabilidad (IMT) contiene la información más actualizada sobre requisitos.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

- Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux. Por ejemplo:

  ```
  Cmnd_Alias SCCMD = /opt/NetApp/snapcenter/scc/bin/scc <non_root_user>
  ALL=(ALL) NOPASSWD:SETENV: SCCMD
  ```

  non_root_user es el nombre del usuario que ha creado y que no es raíz.

## Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de plugins de SnapCenter para Linux.

| Elemento | Requisitos |
| --- | --- |
| Sistemas operativos | • Red Hat Enterprise Linux<br>• Oracle Linux<br>• SUSE Linux Enterprise Server (SLES) |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 2 GB<br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |

| Elemento | Requisitos |
| --- | --- |
| Paquetes de software obligatorios | Tipos de Java 1.8 (64 bits)Oracle Java o OpenJDK<br><br>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta. |

Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp"

## Configure credenciales para los plugins personalizados de SnapCenter

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar los plugins de SnapCenter, y credenciales adicionales para realizar operaciones de protección de datos en sistemas de archivos Windows o bases de datos.

### Lo que necesitará

- Hosts Linux

  Debe configurar credenciales para instalar plugins en hosts Linux.

  Debe configurar las credenciales para el usuario raíz o un usuario que no sea raíz que tenga privilegios sudo para instalar e iniciar el proceso del plugin.

  **Práctica recomendada:** aunque se permite crear credenciales para Linux después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

- Host Windows

  Debe configurar credenciales de Windows antes de instalar plugins.

  Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.

- Aplicaciones de plugins personalizados

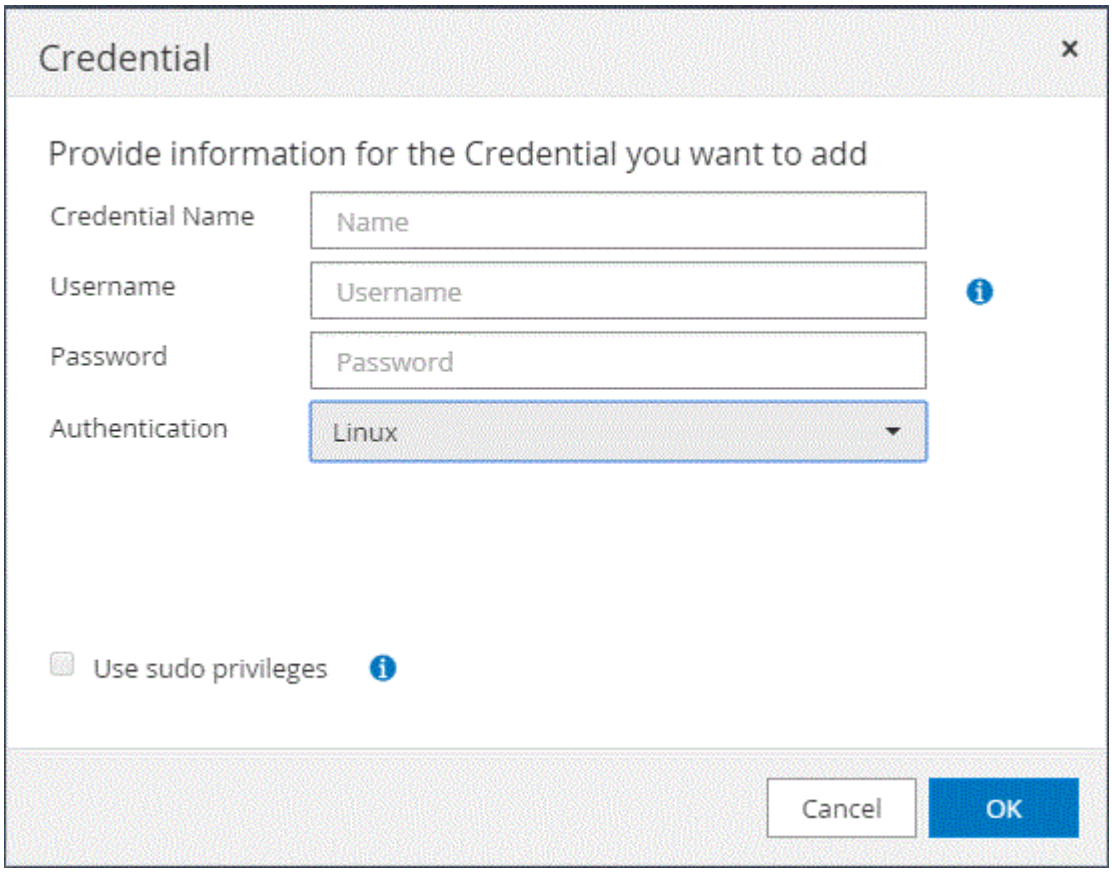
  El plugin utiliza las credenciales seleccionadas o creadas al añadir un recurso. Si un recurso no requiere credenciales durante las operaciones de protección de datos, puede establecer las credenciales como **Ninguno**.

### Acerca de esta tarea

Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al nombre de usuario.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página **Configuración**, haga clic en **credenciales**.
3. Haga clic en **Nuevo**.




4. En la página **Credential**, especifique la información necesaria para configurar las credenciales:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de credencial | Introduzca un nombre para las credenciales. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario | Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.<br>• Administrador de dominio o cualquier miembro del grupo de administradores<br>Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:<br>◦ *NetBIOS\Username*<br>◦ *Domain FQDN\Username*<br>• Administrador local (sólo para grupos de trabajo)<br>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: *Username* |
| Contraseña | Introduzca la contraseña usada para autenticación. |
| Modo de autenticación | Seleccione el modo de autenticación que desea utilizar. |
| Use privilegios sudo | Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz.<br>Aplicable únicamente a usuarios Linux. |

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede que desee asignar mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

## Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

**Lo que necesitará**

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

1. Asigne los privilegios administrativos al GMSA configurado en el host.
2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

   El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

## Instale los plugins personalizados de SnapCenter

### Añada hosts e instale paquetes de plugins en hosts remotos

Es necesario usar la página SnapCenterAdd Host para añadir hosts y, a continuación, instalar los paquetes de plugins. Los plugins se instalan automáticamente en hosts remotos. Puede añadir un host e instalar los paquetes de los plugins para un host individual o para un clúster.

#### Lo que necesitará

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Debe asegurarse de que el servicio de cola de mensajes está en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configurar la cuenta de servicio administrado de grupo en Windows Server 2012 o posterior para

aplicaciones personalizadas"

**Acerca de esta tarea**

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

Si instala plugins en un clúster (WSFC), los plugins se instalan en todos los nodos del clúster.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página **hosts**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de host | Seleccione el tipo de host:<br>• Windows<br>• Linux<br>Los plugins personalizados se pueden utilizar tanto en entornos de Windows como de Linux. |
| Nombre de host | Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.<br>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.<br>En los entornos de Windows, la dirección IP es compatible con los hosts de dominio que no son de confianza solo si se resuelve en el FQDN.<br>Puede introducir las direcciones IP o el FQDN de un host independiente.<br>Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar el FQDN. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Credenciales | Seleccione el nombre de la credencial que ha creado o cree nuevas credenciales.<br><br>Las credenciales deben tener derechos de administración en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales.<br><br>Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado.<br><br>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. |

5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.
6. (Opcional) haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto.<br><br>El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Ruta de instalación | Los plugins personalizados se pueden instalar en un sistema Windows o Linux.<br><br>• En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter.<br><br>Opcionalmente, puede personalizar la ruta.<br><br>• Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter.<br><br>Opcionalmente, puede personalizar la ruta.<br><br>• Para los plugins personalizados de SnapCenter:<br><br>i. En la sección Custom Plug-ins, haga clic en **Browse** y, a continuación, seleccione la carpeta del plugin personalizado comprimida.<br><br>La carpeta comprimida contiene el código del plugin y el archivo .xml del descriptor.<br><br>ii. Haga clic en **cargar**.<br><br>El archivo .xml del descriptor en la carpeta del plugin personalizado comprimida se valida antes de cargar el paquete.<br><br>Aparece la lista de los plugins personalizados que se cargan en el servidor de SnapCenter.<br><br>Si desea gestionar aplicaciones de MySQL o DB2, puede utilizar los plugins personalizados de MySQL y DB2 proporcionados por NetApp. Los plugins personalizados de MySQL y DB2 están disponibles en la "Automation Store de NetApp" |
| Omitir comprobaciones previas a la instalación | Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in | En el caso de host de Windows, seleccione esta casilla de comprobación si desea utilizar una cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de plugin.<br>Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$.<br>GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows. |

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación *Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

   Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en C:\Program Files\NetApp\SnapCenter WebApp para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero debe solucionar el problema.

   En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

1. Si el tipo de host es Linux, verifique la huella digital y, a continuación, haga clic en **Confirmar y enviar**.

   La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

2. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación están en /custom_location/snapcenter/logs.

### Instale paquetes de plugins de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de plugins de SnapCenter para Linux o Windows en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

#### Lo que necesitará

El usuario que agrega un host debe tener derechos administrativos en el host.

- Pasos*

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
3. Instale el plugin en varios hosts mediante el cmdlet Install-SmHostPackage y los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Puede utilizar la opción -skipprecheck cuando haya instalado los plugins manualmente y no quiera validar si el host cumple los requisitos para instalar el plugin.

1. Introduzca sus credenciales para la instalación remota.

**Instale los plugins personalizados de SnapCenter en hosts Linux mediante la interfaz de la línea de comandos**

Debe instalar los plugins personalizados de SnapCenter mediante la interfaz de usuario (UI) de SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar los plugins personalizados en el modo consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

- Pasos*

1. Copie el paquete de plugins de SnapCenter para el archivo de instalación de Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar los plugins personalizados.

   Puede acceder a esta ruta desde el host en el que está instalado el servidor SnapCenter.

2. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el archivo de instalación.
3. Instale el plugin: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT indica el puerto de comunicación HTTPS de SMCore.
   - -DSERVER_IP indica la dirección IP del servidor SnapCenter.
   - -DSERVER_HTTPS_PORT indica el puerto HTTPS del servidor SnapCenter.
   - -DUSER_INSTALL_DIR indica el directorio en el que desea instalar el paquete de plugins de SnapCenter para Linux.
   - DINSTALL_LOG_NAME indica el nombre del archivo de registro.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Añada el host al servidor de SnapCenter con el cmdlet Add-Smhost y los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

5. Inicie sesión en SnapCenter y cargue el plugin personalizado desde la interfaz de usuario o mediante cmdlets de PowerShell.

   Para cargar el plugin personalizado desde la interfaz de usuario, consulte "Añada hosts e instale paquetes de plugins en hosts remotos" sección.

   La ayuda sobre cmdlet de SnapCenter y la información de referencia sobre cmdlet contienen más información acerca de cmdlets de PowerShell.

"Guía de referencia de cmdlets de SnapCenter Software".

### Supervise el estado de la instalación de plugins personalizados

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

#### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
   a. Haga clic en **filtro**.
   b. Opcional: Indique las fechas de inicio y finalización.

c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.

d. En el menú desplegable de estado, seleccione el estado de instalación.

e. Haga clic en **aplicar**.

4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configurar certificado de CA

### Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

> Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

### Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

- Pasos*

1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
2. En la ventana **Agregar o quitar complementos**, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
3. En la ventana del complemento **certificados**, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

| En esta ventana del asistente… | Haga lo siguiente… |
| --- | --- |
| Importar clave privada | Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**. |
| Importar formato de archivo | No realice cambios; haga clic en **Siguiente**. |
| Seguridad | Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**. |
| Finalización del Asistente para importación de certificados | Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación. |

El certificado de importación debe incluirse con la clave privada (los formatos admitidos son: *.pfx, *.p12, *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

**Obtenga la huella digital del certificado de CA**

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

- Pasos*
  1. Realice lo siguiente en la interfaz gráfica de usuario:
     a. Haga doble clic en el certificado.
     b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
     c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
     d. Copie los caracteres hexadecimales del cuadro.
     e. Quite los espacios entre los números hexadecimales.

        Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

  2. Realice lo siguiente desde PowerShell:
     a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

        *Get-ChildItem -Path Cert:\LocalMachine\My*

     b. Copie la huella digital.

**Configure el certificado de CA con servicios de plugins de host de Windows**

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan

implementado certificados de CA.

- Pasos*

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

   Por ejemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Enlace el certificado recientemente instalado con los servicios de
   plugins del host de Windows mediante la ejecución de los siguientes
   comandos:
   ```

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid"
   ```

   Por ejemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

### Configure el certificado de CA para el servicio de plugins personalizados de SnapCenter en el host Linux

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* tanto como en su almacén de confianza como en su almacén de claves.

#### Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

- Pasos*

1. Puede recuperar la contraseña predeterminada del almacén de claves del plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

Es el valor correspondiente a la clave 'KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

```
 keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña para todos los alias de las entradas de clave
privada en el almacén de claves por la misma contraseña utilizada
para el almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

3. Reinicie el servicio después de cambiar la contraseña.

La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

**Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado**

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado: /Opt/NetApp/snapcenter/scc/etc.
  2. Busque el archivo 'keystore.jks'.
  3. Enumere los certificados añadidos al almacén de claves:

     ```
     keytool -list -v -keystore keystore.jks
     ```

  4. Añada un certificado raíz o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza del plugin personalizado.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

**Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado**

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado /opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Agregue el certificado de CA con clave pública y privada.

   ```
   keytool -importkeystore -srckeystore
   /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore
   keystore.jks -deststoretype JKS
   ```

5. Enumere los certificados añadidos al almacén de claves.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Si el nombre del alias del certificado de CA es largo y contiene
   espacio o caracteres especiales ("*",","), cambie el nombre del alias
   por un nombre simple:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias
   "simple_alias" -keystore keystore.jks
   . Configure el nombre del alias del certificado de CA en el archivo
   agent.properties.
   ```

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

8. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

#### Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

### Acerca de esta tarea

- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es '

opt/NetApp/snapcenter/scc/etc/crl'.

- Pasos*

1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

   Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

### Configure el certificado de CA para el servicio de plugins personalizados de SnapCenter en el host de Windows

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*, tanto como su almacén de confianza como su almacén de claves.

#### Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

- Pasos*

1. Puede recuperar la contraseña predeterminada del almacén de claves del plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

   Es el valor que corresponde a la clave *KEYSTORE_PASS*.

2. Cambie la contraseña del almacén de claves:

   *keytool -storepasswd -keystore.jks*

   > Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool por su ruta completa.

   *C:\Archivos de programa\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore.jks*

3. Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves:

   *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

1. Reinicie el servicio después de cambiar la contraseña.

   > La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

#### Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

   *keytool -list -v -keystore.jks*

4. Añada un certificado raíz o intermedio:

   *Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks*

5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza del plugin personalizado.

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

#### Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo *keystore.jks*.
3. Enumere los certificados añadidos al almacén de claves:

   *keytool -list -v -keystore.jks*

4. Agregue el certificado de CA con clave pública y privada.

   *Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -deststoretype JKS*

5. Enumere los certificados añadidos al almacén de claves.

   *keytool -list -v -keystore.jks*

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

*Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks*

1. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

2. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

#### Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

**Acerca de esta tarea**

- Para descargar el último archivo CRL del certificado de CA relacionado, consulte "Cómo actualizar el archivo de lista de revocación de certificados en el certificado de CA de SnapCenter".
- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es *'C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la CLAVE CRL_PATH.
  2. Puede colocar más de un archivo CRL en este directorio.

     Los certificados entrantes se verificarán en cada CRL.

### Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

**Lo que necesitará**

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

**Después de terminar**

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

# Prepárese para la protección de datos

## Requisitos previos para usar los plugins personalizados de SnapCenter

Antes de usar los plugins personalizados de SnapCenter, el administrador de SnapCenter debe instalar y configurar SnapCenter Server, así como ejecutar las tareas especificadas en los requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en el servidor SnapCenter.
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento y creando credenciales, si es necesario.
- Añada hosts, e instale y cargue los plugins.
- Si corresponde, instale Java 1.7 o Java 1.8 en el host del plugin.
- Si tiene varias rutas de datos (LIF) o una configuración de dNFS, puede realizar lo siguiente mediante la CLI de SnapCenter en el host de la base de datos:
  - De forma predeterminada, todas las direcciones IP del host de la base de datos se añaden a la directiva de exportación de almacenamiento de NFS en la máquina virtual de almacenamiento (SVM) para los volúmenes clonados. Si desea contar con una dirección IP específica o restringir a una subred de direcciones IP, ejecute la CLI de Set-PreferredHostIPsInStorageExportPolicy.
  - Si tiene varias LIF en las SVM, SnapCenter elije la ruta de LIF correspondiente para montar el volumen clonado de NFS. No obstante, si desea especificar una determinada ruta de LIF, debe ejecutar la CLI de Set-SvmPreferredDataPath. La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".
- Configure SnapMirror y SnapVault si quiere realizar una replicación de backup.
- Asegúrese de que el puerto 9090 no esté en uso en otra aplicación del host.

  El uso del puerto 9090 debe reservarse a los plugins personalizados de SnapCenter, junto con los otros puertos requeridos por SnapCenter.

## Cómo se usan los recursos, los grupos de recursos y las políticas para proteger los recursos de los plugins personalizados

Antes de usar SnapCenter, es necesariol comprender ciertos conceptos básicos vinculados con las operaciones de backup, clonado y restauración que se ejecutan. El

usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos generalmente son bases de datos, sistemas de archivos de Windows o máquinas virtuales que se incluyen en un backup o se clonan con SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupacion de recursos en un host o un clúster.

  Al realizar una operación con un grupo de recursos, esta se ejecuta en los recursos definidos en el grupo de acuerdo con la programación que se especificó para dicho grupo de recursos.

  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

- Las políticas especifican la frecuencia de backup, la retención de copias, la replicación, los scripts y otras características de las operaciones de protección de datos.

  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. Asimismo, puede seleccionar una política al realizar un backup bajo demanda para un recurso individual.

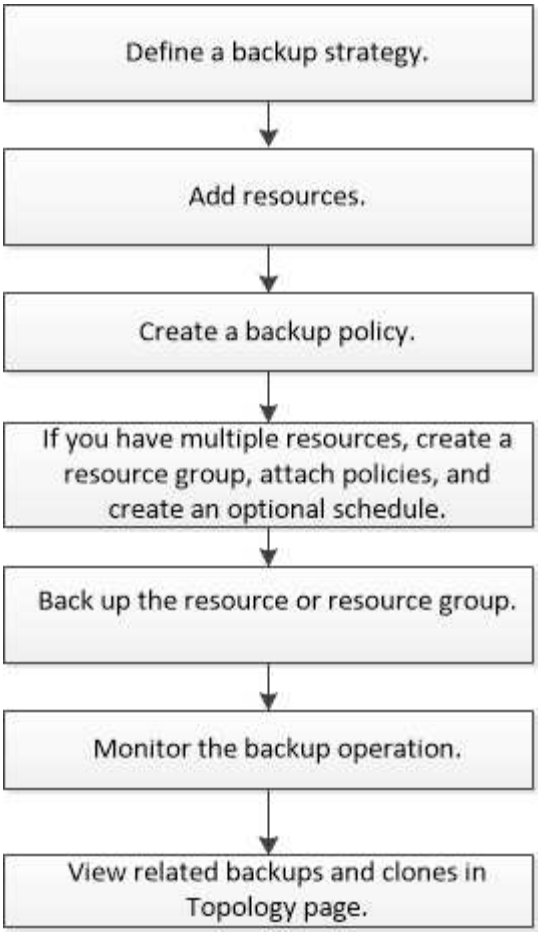
Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos o todos los sistemas de archivos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando crea el grupo de recursos y añade las políticas, puede configurar el grupo de recursos para que ejecute un backup diario basado en archivos y otra programación que ejecute un backup por hora basado en Snapshot.

# Realice backup de recursos de plugins personalizados

## Realice backup de recursos de plugins personalizados

El flujo de trabajo de backup incluye planificar, identificar los recursos para el backup, gestionar las políticas de backup, crear grupos de recursos y añadir políticas, crear backups y supervisar las operaciones.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software"

## Añada recursos a los plugins personalizados de SnapCenter

Debe añadir los recursos que desee incluir en un backup o clonar. En función de su entorno, los recursos pueden ser instancias de una base de datos o recopilaciones que desee clonar o incluir en un backup.

### Lo que necesitará

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir credenciales.
- Debe haber creado un plugin personalizado.

  "Desarrolle un complemento para la aplicación"

- Debe haber cargado los plugins en SnapCenter Server.

### Acerca de esta tarea

También puede añadir recursos para MySQL y aplicaciones DB2. Estos plugins pueden descargarse del "Almacén de automatización del almacenamiento de NetApp".

- Pasos*

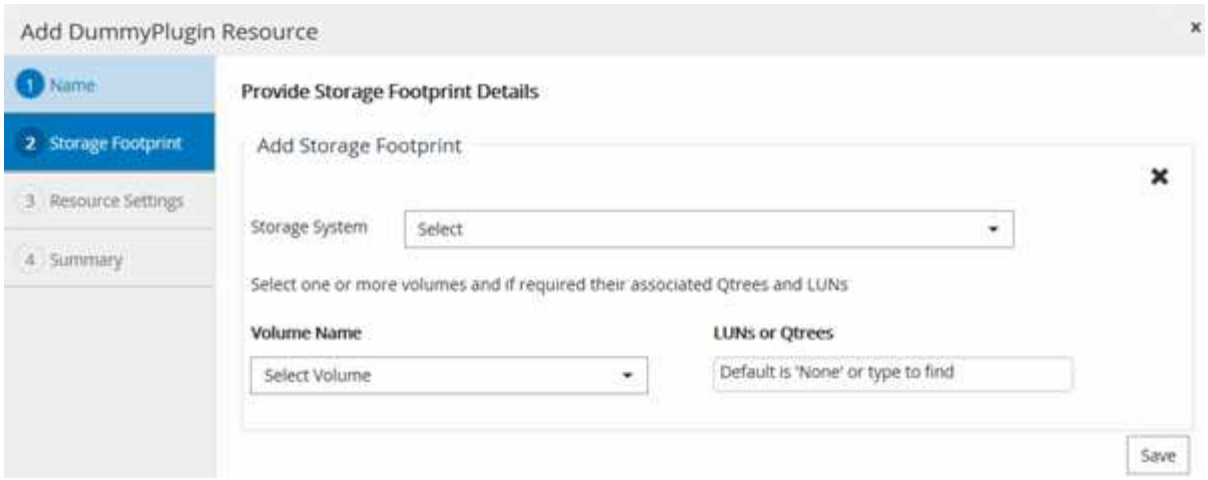
1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, haga clic en **Agregar recurso**.
3. En la página **proporcionar detalles del recurso**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba el nombre del recurso. |
| Nombre de host | Seleccione el host. |
| Tipo | Seleccione el tipo. El usuario define el tipo según el archivo de descripción del plugin. Por ejemplo, base de datos e instancia.<br><br>Si el tipo seleccionado tiene un elemento principal, escriba los detalles de dicho elemento. Por ejemplo, si el tipo es una base de datos y el elemento principal es una instancia, escriba los detalles de la instancia. |
| Nombre de credencial | Seleccione Credential o cree una credencial nueva. |
| Monte las rutas | Escriba las rutas de montaje en el punto donde se monta el recurso. Solo corresponde a un host Windows. |

4. En la página **Provide Storage Footprint**, seleccione un sistema de almacenamiento y elija uno o más volúmenes, LUN y qtrees; a continuación, haga clic en **Save**.

   Opcional: Haga clic en el Icono para añadir más volúmenes, LUN y qtrees desde otros sistemas de almacenamiento.

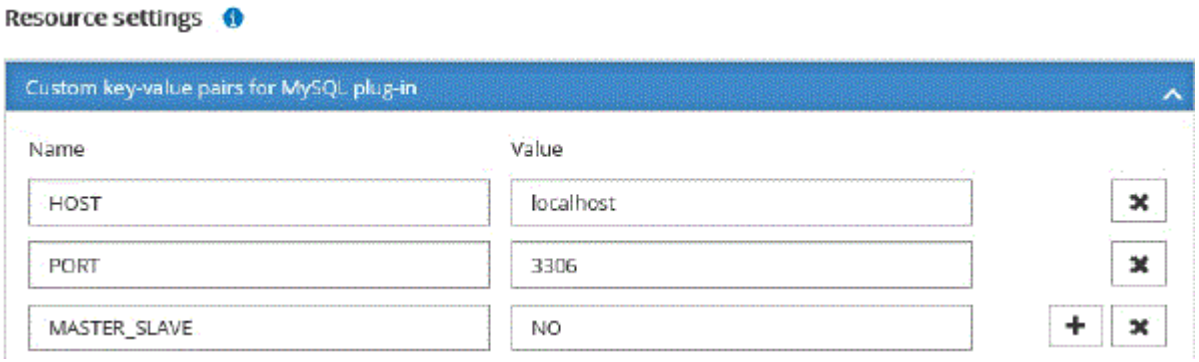
   Los plugins personalizados de SnapCenter no admiten la detección automática de los recursos y detalles de almacenamiento correspondientes a los entornos físicos y virtuales. Debe proporcionar la información de almacenamiento de los entornos físico y virtual durante la creación de los recursos.




5. En la página **Configuración de recursos**, proporcione pares personalizados de clave-valor para el recurso.

   Use estos pares si desea pasar información específica del recurso. Por ejemplo, al utilizar el complemento MySQL, debe especificar UN HOST como HOST=nombre de host, PUERTO =puerto-no utilizado para la configuración MySQL y maestro/esclavo COMO MAESTRO_ESCLAVO = "'SÍ'" o "'NO'" (el nombre es MASTER_SLAVE y el valor es "'SÍ'" o "'NO'").

   Asegúrese de que las palabras HOST y PUERTO estén en mayúsculas.




1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

**resultado**

Los recursos se muestran junto con cierta información, como el tipo, el host o el nombre de clúster, las políticas y los grupos de recursos asociados, y el estado general.

**Después de terminar**

Si desea proporcionar acceso a los activos a otros usuarios, el administrador de SnapCenter debe realizar la asignación. De este modo, los usuarios pueden realizar las acciones para las cuales tienen permisos sobre los activos que les asignaron.

Después de añadir los recursos, puede modificar sus detalles. Si un recurso de plugin personalizado tiene backups asociados, no se pueden modificar los siguientes campos: Nombre del recurso, tipo de recurso y nombre de host.

## Crear políticas para recursos de plugins personalizados

Antes de usar SnapCenter para realizar un backup de recursos específicos de un plugin personalizado, debe crear una política de backup para el recurso o el grupo de recursos que incluirá en el backup.

**Lo que necesitará**

- Debe tener definida una estrategia de backup.

  Para obtener detalles, consulte la información sobre cómo definir una estrategia de protección de datos para plugins personalizados.

- Debe tener preparada la protección de datos.

  La preparación de la protección de datos incluye instalar SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir recursos.

- Debe asignar las máquinas virtuales de almacenamiento (SVM) para operaciones de mirroring o almacén.

  El administrador de SnapCenter debe haberle asignado las instancias de SVM de los volúmenes de origen y de destino en caso de que replique copias de Snapshot en un reflejo o almacén.

- Debe añadir manualmente los recursos que desee proteger.

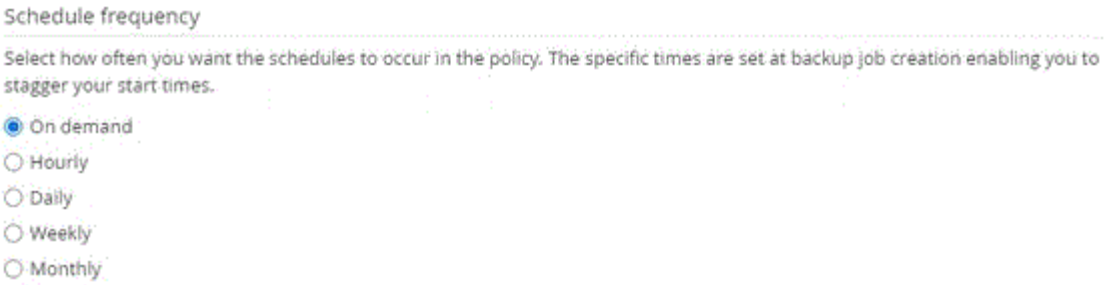
**Acerca de esta tarea**

- Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups. De forma adicional, puede definir la configuración de replicación, script y aplicaciones.
- Puede especificar opciones en la política para ahorrar tiempo cuando desee reutilizarla con otro grupo de recursos.
- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página **Configuración**, haga clic en **Directivas**.
  3. Haga clic en **Nuevo**.
  4. En la página **Nombre**, introduzca el nombre y la descripción de la directiva.
  5. En la página **Configuración**, realice los siguientes pasos:

     - Especifique el tipo de programa seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

       Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de backup mientras crea un grupo de recursos. De este modo, puede crear grupos de recursos que compartan la misma política y la misma frecuencia de backup, pero también asignar diferentes programaciones de backup a cada política.




Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

- En la sección **Configuración de copia de seguridad personalizada**, proporcione cualquier configuración de copia de seguridad específica que deba pasarse al plugin en formato clave-valor. Puede pasar varios pares de clave-valor al plugin.

1. En la página **Retention**, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página Tipo de copia de seguridad:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Conservar una cierta cantidad de copias de Snapshot | Seleccione **total Snapshot copies to keep** y, a continuación, especifique el número de copias Snapshot que desea conservar.<br><br>Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas.<br><br>Debe establecer el número de retención en 2 o un valor más alto si tiene pensado habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino.<br><br>El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Conserve las copias de Snapshot por una cierta cantidad de días | Seleccione **mantener copias Snapshot para** y, a continuación, especifique el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas. |

2. En la página **replicación**, especifique la configuración de replicación:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Actualizar SnapMirror después de crear una copia Snapshot local** | Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror).<br><br>Si la relación en ONTAP es del tipo Mirror/Vault y solo se selecciona esta opción, la copia de Snapshot creada en el origen no se transferirá al destino, pero figurará en el destino. Si esta copia de Snapshot se selecciona del destino con el fin de realizar una operación de recuperación, aparece un mensaje de error indicando que la ubicación secundaria no está disponible para el backup reflejado/en almacenamiento. |
| **Actualizar SnapVault después de crear una copia Snapshot local** | Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). |
| **Etiqueta de política secundaria** | Seleccione una etiqueta de Snapshot.<br><br>Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta.<br><br>Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Número de reintentos de error** | Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga. |

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Crear grupos de recursos y añadir políticas

Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación. Un grupo de recursos es necesario para cualquier trabajo de protección de datos. También debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, haga clic en Nuevo grupo de recursos.
3. En la página **Nombre**, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba un nombre para el grupo de recursos.<br>El nombre del grupo de recursos no debe superar los 250 caracteres. |
| Etiquetas | Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.<br>Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.<br><br>Por ejemplo, *customtext_resource group_policy_hostname o resource group_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |

4. Opcional: En la página **Recursos**, seleccione un nombre de host de la lista desplegable **Host** y el tipo de recurso de la lista desplegable **Tipo de recurso**.

   Esto permite filtrar información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. Opcional: En la página **Configuración de la aplicación**, haga lo siguiente:

   a. Haga clic en la flecha backups para establecer las opciones de backup adicionales.

      Habilite el backup del grupo de consistencia y realice las siguientes tareas:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Permitir que se complete la operación de snapshot del grupo de consistencia | Seleccione Urgent, Medium o Relaxed para especificar el tiempo de espera hasta completar la operación de la copia de Snapshot.<br><br>Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos. |
| Deshabilite la sincronización WAFL | Seleccione este campo para evitar forzar un punto de coherencia de WAFL. |

+

a. Haga clic en la flecha Scripts y escriba los comandos previos y posteriores para el modo de inactividad, copia de Snapshot y la reanudación de la copia. También puede escribir los comandos previos para que se ejecuten antes de salir en caso de un fallo.

b. Haga clic en la flecha Custom Configurations y utilice este recurso para escribir los pares personalizados clave-valor requeridos en todas las operaciones de protección de datos.

| Parámetro | Ajuste | Descripción |
|---|---|---|
| ARCHIVE_LOG_ENABLE | (S/N) | Permite la gestión del registro de archivos para eliminar los registros de archivos. |
| RETENCIÓN_LOG_ARCHIVO | número_de_días | Especifica la cantidad de días que se conservan los registros de archivo.<br><br>Este valor debe ser igual o mayor que las RETENTIONS NTAP_SNAPSHOT_. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Especifica la ruta de acceso al directorio que contiene los registros de archivo. |

| Parámetro | Ajuste | Descripción |
|---|---|---|
| ARCHIVO_LOG_EXT | extensión_archivo | Especifica la longitud de la extensión del archivo de registro de archivos.<br><br>Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.161518551942 9 y si el valor file_extension es 5, la extensión del registro conservará 5 dígitos, que son 16151. |
| ARCO ARCHIVE_LOG_RECURSIVE_SE | (S/N) | Permite la gestión de registros de ficheros en subdirectorios.<br><br>Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios. |

c. Haga clic en la flecha **Snapshot Copy Tool** para seleccionar la herramienta que permite crear copias Snapshot:

| Si desea que… | Realice lo siguiente… |
|---|---|
| SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente antes de crear una copia de Snapshot. En el caso de recursos de Linux, esta opción no es aplicable. | Seleccione SnapCenter with File System Consistency.<br><br>Esta opción no es aplicable para el plugin de SnapCenter para la base de datos SAP HANA. |
| SnapCenter cree una copia de Snapshot en el nivel del almacenamiento | Seleccione SnapCenter without File System Consistency. |
| Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot. | Seleccione Other y escriba el comando que se ejecutará en el host a fin de crear una copia de Snapshot. |

7. En la página **Directivas**, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.

También puede crear una directiva haciendo clic en + .

Las directivas se enumeran en la sección **Configurar horarios para directivas seleccionadas**.

a. En la columna **Configurar horarios**, haga clic en + para la directiva que desea configurar.

b. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y haga clic en OK.

   Policy_name es el nombre de la política seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules. No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

1. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Realice backup de recursos de plugins individuales

Si un recurso de un plugin individual no forma parte de ningún grupo de recursos, puede incluirlo en el backup mediante la página Resources. Puede realizar el backup del recurso bajo demanda, o bien, si el recurso tiene una política anexada y una programación configurada, el backup se realiza automáticamente según esa programación.

**Lo que necesitará**

- Debe tener creada una política de backup.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

     Haga clic en y, a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.

  3. Haga clic en el recurso que desea incluir en el backup.
  4. En la página **recurso**, si desea utilizar un nombre personalizado, active la casilla de verificación **usar formato de nombre personalizado para copia Snapshot** y, a continuación, escriba un formato de nombre personalizado para el nombre de copia Snapshot.

     Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.

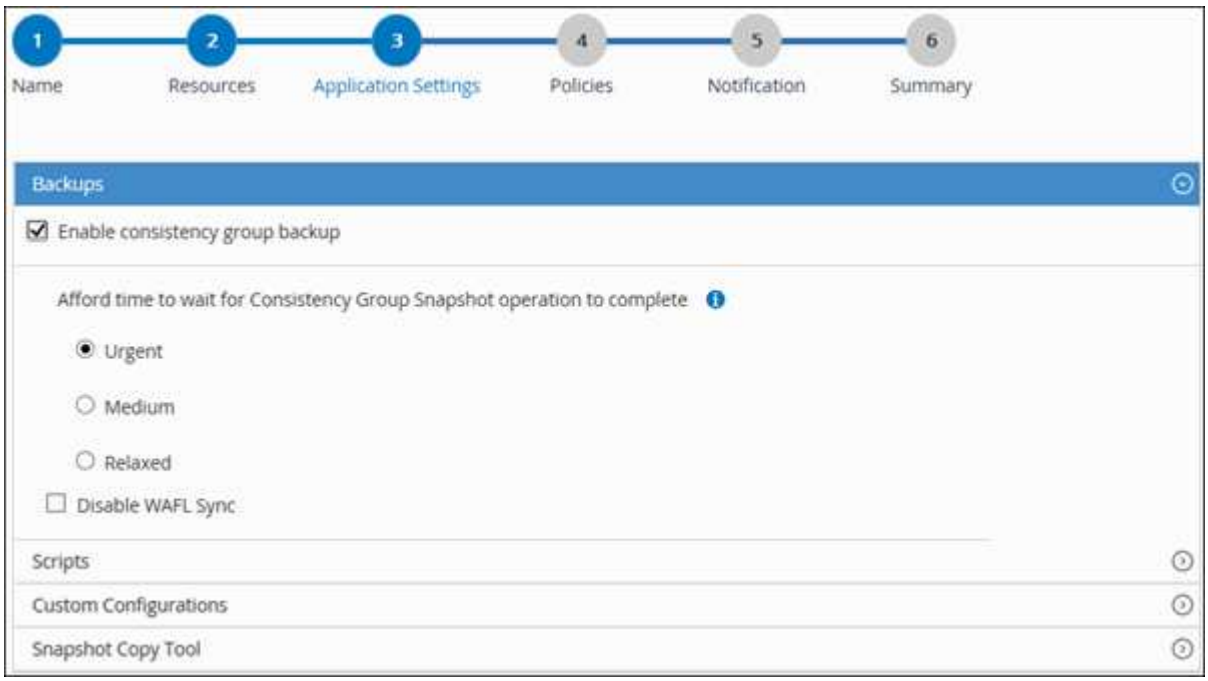
  5. En la página **Configuración de la aplicación**, haga lo siguiente:

     a. Haga clic en la flecha **copias de seguridad** para establecer las opciones de copia de seguridad adicionales:

Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Permitir que se complete la operación de snapshot del grupo de consistencia | Seleccione Urgent, Medium o Relaxed para especificar el tiempo de espera hasta completar la operación de la copia de Snapshot.<br><br>Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos. |
| Deshabilite la sincronización WAFL | Seleccione este campo para evitar forzar un punto de coherencia de WAFL. |

+




a. Haga clic en la flecha **Scripts** para ejecutar comandos previos y posteriores para la pausa, la copia de Snapshot y la reanudación de la copia. También puede ejecutar los comandos previos antes de salir de la operación de backup.

   Los scripts previos y posteriores se ejecutan en el servidor de SnapCenter.

b. Haga clic en la flecha **configuraciones personalizadas** y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.

c. Haga clic en la flecha **Snapshot Copy Tool** para seleccionar la herramienta que permite crear copias Snapshot:

| Si desea que… | Realice lo siguiente… |
| --- | --- |
| SnapCenter debe tomar una copia de Snapshot en el nivel del almacenamiento | Seleccione **SnapCenter sin coherencia del sistema de archivos**. |

| Si desea que… | Realice lo siguiente… |
| --- | --- |
| SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente para luego crear una copia de Snapshot | Seleccione **SnapCenter with File System Consistency**. |
| Se escriba el comando para crear una copia de Snapshot | Seleccione **otros** y, a continuación, escriba el comando para crear una copia Snapshot. |

6. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

   También puede crear una política haciendo clic en + .

   En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   a. Haga clic en + En la columna Configure Schedules correspondiente a la política para la cual se desea configurar una programación.

   b. En el cuadro de diálogo Agregar programas para la directiva *policy_name* , configure la programación y, a continuación, haga clic en **Aceptar**.

      Donde, *policy_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

1. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

2. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de los recursos.

3. Haga clic en **copia de seguridad ahora**.
4. En la página Backup, realice los siguientes pasos:

   a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Realice un backup de grupos de recursos de plugins personalizados

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

**Lo que necesitará**

- Debe tener creado un grupo de recursos con una política anexada.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «incluir toda la copia reflejada». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione **Grupo de recursos** en la lista **Ver**.

   Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en y seleccionando la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. En la página **grupos de recursos**, seleccione el grupo de recursos del que desea realizar la copia de seguridad y, a continuación, haga clic en **realizar copia de seguridad ahora**.
4. En la página **copia de seguridad**, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.
   - En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

     "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"

   - Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup. Para aumentar el tamaño de pila de Java, busque el archivo de script /opt/netapp/init_scripts/scvservice. En ese script, la `do_start method` Command inicia el servicio de plugin de VMware de SnapCenter. Actualice este comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

## Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los

cmdlets de PowerShell para realizar operaciones de protección de datos.

**Lo que necesitará**

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

  No debe haber instalaciones de complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

  SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de gestión única.

- Pasos*

1. Inicie una sesión de conexión de PowerShell con mediante el cmdlet Open-SmConnection.

   En este ejemplo, se abre una sesión de PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Cree una nueva conexión con el sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

   En este ejemplo, se crea una nueva conexión con el sistema de almacenamiento:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Cree una credencial nueva mediante el cmdlet Add-SmCredential.

   En este ejemplo, se crea una nueva credencial llamada FinanceAdmin con las credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Realizar backup de recursos con cmdlets de PowerShell

El backup de un recurso implica establecer una conexión con SnapCenter Server, añadir recursos, añadir una política, crear una política de recursos de backup y realizar el backup.

### Lo que necesitará

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe añadir la conexión con el sistema de almacenamiento y crear una credencial.

### Acerca de esta tarea

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
   ```

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada los recursos mediante el cmdlet Add-SmResources.

   En este ejemplo, se añaden recursos:

   ```
   Add-SmResource -HostName '10.232.206.248' -PluginCode 'DB2'
   -ResourceName NONREC1 -ResourceType Database -StorageFootPrint ( @
   {"VolumeName"="DB2_NONREC1DB";"LunName"="DB2_NONREC1DB";"Vserver"="vs
   erver_scauto_secondary"}) -Instance db2inst1
   ```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.

   En este ejemplo, se crea una nueva política de backup:

   ```
   Add-SMPolicy -PolicyName 'db2VolumePolicy' -PolicyType 'Backup'
   -PluginPolicyType DB2  -description 'VolumePolicy'
   ```

4. Añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

   En este ejemplo, se crea un nuevo grupo de recursos con la política y los recursos especificados:

```
Add-SmResourceGroup -ResourceGroupName
'Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix' -Resources
@(@
{"Host"="10.232.206.248";"Uid"="db2inst2\NONREC"},@{"Host"="10.232.20
6.248";"Uid"="db2inst1\NONREC"}) -Policies db2ManualPolicy
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix -Policy
db2ManualPolicy
```

6. Consulte el estado del trabajo de backup mediante el cmdlet Get-SmBackupReport.

   Este ejemplo muestra un informe con un resumen de todos los trabajos realizados en la fecha especificada:

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

## Supervisar las operaciones de backup de los recursos de plugins personalizados

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Jobs**.
3. En la página Jobs, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
   d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
   e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

   Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

## Cancelar las operaciones de backup para plugins personalizados

Es posible cancelar las operaciones de backup que se encuentran en cola.

### Lo que necesitará

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones.

- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o el panel **Activity**.
- No es posible cancelar una operación de backup en ejecución.
- Es posible utilizar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de backup.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.
- Pasos*

1. Ejecute una de las siguientes acciones:

| Del… | Acción |
|---|---|
| Página Monitor | a. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**.<br>b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**. |
| Panel de actividades | a. Tras iniciar la operación de backup, haga clic en En el panel Activity para ver las cinco operaciones más recientes.<br>b. Seleccione la operación.<br>c. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**. |

Se cancela la operación y el recurso se revierte al estado anterior.

## Consulte los clones y backups relacionados con los recursos de plugins personalizados en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario. En la página Topology, es posible ver todos los backups y clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

### Acerca de esta tarea

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
-

Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.

Los clones de un backup de un reflejo de versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejos de la vista de topología no incluye el backup de versión flexible.

- Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

  La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

  Los clones de un backup de un reflejo de versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejos de la vista de topología no incluye el backup de versión flexible.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

   Si el recurso está protegido, se muestra la página con el resumen seleccionado.

4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el almacenamiento principal y secundario.

   La sección Summary Card muestra la cantidad total de backups y clones.

   Al hacer clic en el botón de actualización, se inicia una consulta del almacenamiento para ver un número preciso.

5. En la vista **Administrar copias**, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

   Estos detalles se muestran en forma de tabla.

6. Seleccione el backup en la tabla y haga clic en los iconos de protección de datos para realizar operaciones de restauración, clonado, cambio de nombre y eliminación.

   Los backups que figuran en el sistema de almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

Los backups que figuran en el sistema de almacenamiento principal no pueden cambiar de nombre.

1. Si desea eliminar un clon, selecciónelo en la tabla y haga clic en para eliminar el clon.

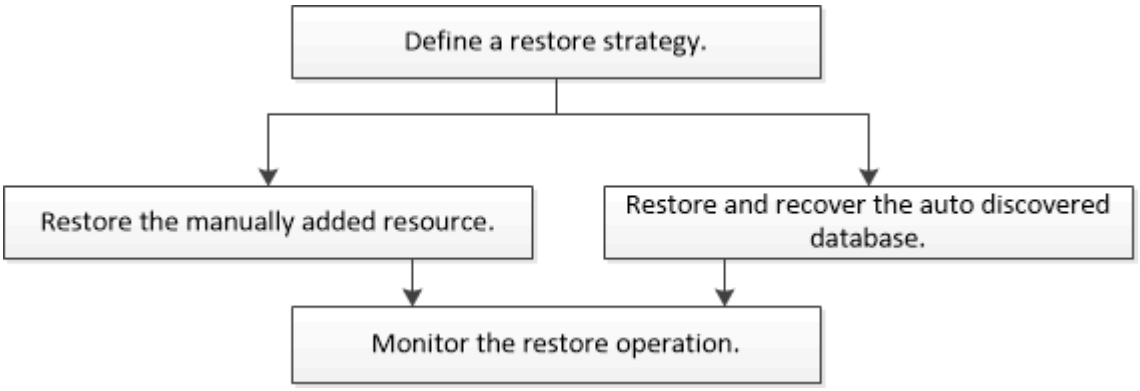
# Restaure recursos de plugins personalizados

## Restaure recursos de plugins personalizados

El flujo de trabajo de restauración y recuperación incluye planificar, realizar las operaciones de restauración y supervisarlas.

### Acerca de esta tarea

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de restauración:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. Para obtener información sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software".

## Restaurar un backup de recursos

Es posible usar SnapCenter para restaurar recursos. Las capacidades de las operaciones de restauración dependen del plugin que se use.

### Lo que necesitará

- Debe tener un backup de los recursos o del grupo de recursos.
- El administrador de SnapCenter asignó SVM para los volúmenes de origen y los volúmenes de destino si va a replicar copias de Snapshot a un reflejo o un almacén.
- Cancele la operación de backup que se encuentra en curso y que corresponde al recurso o grupo de recursos que desea restaurar.

### Acerca de esta tarea

La operación de restauración predeterminada solo restaura objetos del almacenamiento. Las operaciones de restauración en el nivel de la aplicación solo pueden realizarse si el plugin personalizado incluye dicha capacidad.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Los recursos se muestran junto con cierta información, como el tipo, el host o el nombre de clúster, las políticas y los grupos de recursos asociados, y el estado.

   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

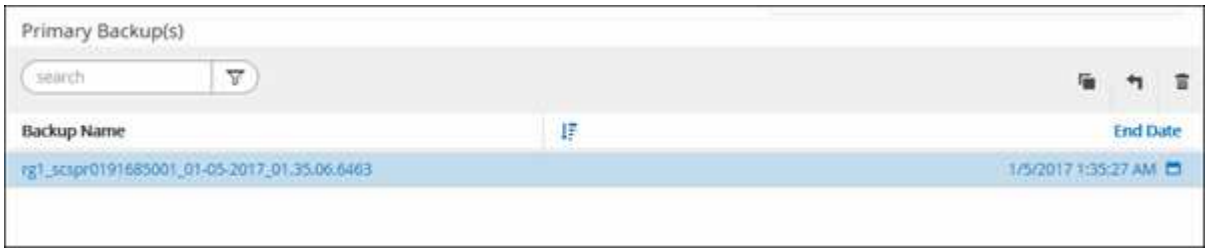
   Si el recurso no está protegido, se muestra *not protected* en la columna **Overall Status**.

El estado *not protected* en la columna **Overall Status** puede significar que el recurso no está protegido o que un usuario diferente hizo una copia de seguridad del recurso.

1. Seleccione el recurso, o bien seleccione un grupo de recursos y, a continuación, elija un recurso de ese grupo.

   Se muestra la página con el resumen.

2. En la vista **Manage Copies**, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
3. En la tabla de backups primarios, seleccione el backup desde el cual quiere restaurar y, a continuación, haga clic en .




4. En la página **Restore Scope**, seleccione **Complete Resource** o **File Level**.
   a. Si seleccionó **Complete Resource**, se restaura la copia de seguridad del recurso.

      Si el recurso contiene volúmenes o qtrees como Storage Footprint, entonces las copias de Snapshot más recientes, como los volúmenes o qtrees, se eliminan y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

   b. Si ha seleccionado **nivel de archivo**, puede seleccionar **todo** o seleccionar volúmenes o qtrees y, a continuación, introducir la ruta relacionada con los volúmenes o qtrees que se seleccionan separados por comas.
      - Puede seleccionar varios volúmenes y qtrees.
      - Si el tipo de recurso es LUN, se restaura el LUN completo. Puede seleccionar varios LUN. + NOTA: Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.
5. En la página **Tipo de recuperación**, realice los siguientes pasos: Seleccione la opción para aplicar registros. Asegúrese de que el plugin admite todos los registros y registros hasta que el tipo de

restauración antes de seleccionarlo.

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Restaurar todos los registros | Seleccione **todos los registros**. Asegúrese de que el plugin admite **todos los registros**. |
| Restaure todos los registros hasta la hora especificada | Seleccione **registros hasta**. Asegúrese de que el plugin admite **registros hasta**. |
| Restaure el backup de recursos | Seleccione **Ninguno**. |

6. En la página **Pre OPS**, escriba los comandos previos a la restauración y los comandos de desmontaje que se ejecutarán antes de realizar un trabajo de restauración.
7. En la página **Post OPS**, escriba los comandos Mount y post restore que se ejecutarán después de realizar un trabajo de restauración.
8. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en la página **Ajustes** > **Ajustes globales**.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Supervisar las operaciones de restauración de recursos de plugins personalizados

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

**Acerca de esta tarea**

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

# Clonar backups de recursos de plugins personalizados

## Clonar backups de recursos de plugins personalizados

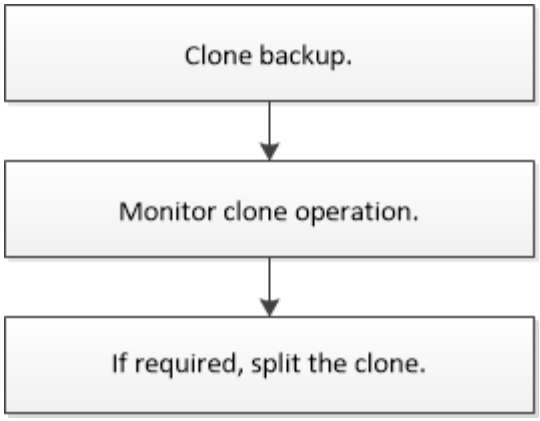
El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

### Acerca de esta tarea

Es posible clonar backups de recursos por los siguientes motivos:

- Para probar la funcionalidad que debe implementarse mediante la estructura de recursos actuales y el contenido durante los ciclos de desarrollo de aplicaciones
- Para herramientas de manipulación y extracción de datos cuando se rellenan almacenes de datos
- Para recuperar datos que se eliminaron o se modificaron por error

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de clonado:




También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software".

## Clonar desde un backup

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario. Las capacidades de las operaciones de clonado dependen del plugin que se use.

**Lo que necesitará**

- Debe tener un backup de los recursos o del grupo de recursos.
- La operación de clonado predeterminada solo clona objetos del almacenamiento. Las operaciones de clonado en el nivel de la aplicación solo pueden realizarse si el plugin personalizado incluye dicha capacidad.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Los recursos se muestran junto con cierta información, como el tipo, el host o el nombre de clúster, las políticas y los grupos de recursos asociados, y el estado.
3. Seleccione el recurso o el grupo de recursos.

   Debe seleccionar un recurso para seleccionar un grupo de recursos.

   Se muestra la página con el resumen o grupo de recursos.
4. En la vista **Manage Copies**, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. Seleccione el backup de datos de la tabla y haga clic en .
6. En la página Locations, realice lo siguiente:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Clone el servidor | De forma predeterminada, se llena el host de origen.<br><br>Si desea especificar otro host, seleccione el host donde debe montarse el clon y donde esté instalado el plugin. |
| Sufijo de clon | Es obligatorio cuando el destino y el origen del clon son iguales.<br><br>Escriba un sufijo que se anexará al nombre del recurso recién clonado. El sufijo garantiza que el recurso clonado sea único en el host.<br><br>Por ejemplo, rs1_clone. Si clona en el mismo host que el recurso original, debe proporcionar un sufijo para diferenciar el recurso clonado del original; de lo contrario, se producirá un error en la operación. |

Si el recurso seleccionado es un LUN y se está clonando a partir de un backup secundario, se muestran los volúmenes de destino. Un único origen puede tener varios volúmenes de destino.

7. En la página **Configuración**, realice lo siguiente:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre del iniciador | Escriba el nombre del iniciador del host, que es IQDN o WWPN. |
| Protocolo de iGroup | Seleccione el protocolo de iGroup. |

La página Settings se muestra solo si el tipo de almacenamiento es un LUN.

8. En la página **Scripts**, escriba los comandos para el clon previo o posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente. Escriba el comando de montaje para montar un sistema de archivos en un host.

   Por ejemplo:

   - Comando previo a la clonado: Elimine las bases de datos existentes con el mismo nombre
   - Comando posterior a la clonado: Verifique o inicie una base de datos.

     Comando de montaje para un volumen o qtree en una máquina Linux: Lcódigo <VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

9. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo.

10. Revise el resumen y haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Clonar backups mediante cmdlets de PowerShell

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

**Lo que necesitará**

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Para obtener información sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Enumere los backups que pueden clonarse mediante el cmdlet Get-SmBackup o Get-SmResourceGroup.

   Este ejemplo muestra información sobre todos los backups disponibles:

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
   1              Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                    Full Backup
   2              Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

   En este ejemplo, se muestra información sobre un grupo de recursos especificado:

```
PS C:\> Get-SmResourceGroup

    Description                 :
    CreationTime                : 10/10/2016 4:45:53 PM
```

```
    ModificationTime            : 10/10/2016 4:45:53 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               :
SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Completed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassCredential            : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
    IsInternal                  : False
    EnableEmailAttachment       : False
    VerificationSettings        : {}
    Name                        : NFS_DB
    Type                        : Group
    Id                          : 2
    Host                        :
    UserName                    :
    Passphrase                  :
    Deleted                     : False
    Auth                        : SMCoreContracts.SmAuth
    IsClone                     : False
    CloneLevel                  : 0
    Hosts                       :
    StorageName                 :
    ResourceGroupNames          :
    PolicyNames                 :

    Description                 :
```

```
    CreationTime                : 10/10/2016 4:51:36 PM
    ModificationTime            : 10/10/2016 5:27:57 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               :
SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Failed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassRunAs                 : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
    IsInternal                  : False
    EnableEmailAttachment       : False
    VerificationSettings        : {}
    Name                        : Test
    Type                        : Group
    Id                          : 3
    Host                        :
    UserName                    :
    Passphrase                  :
    Deleted                     : False
    Auth                        : SMCoreContracts.SmAuth
    IsClone                     : False
    CloneLevel                  : 0
    Hosts                       :
    StorageName                 :
    ResourceGroupNames          :
    PolicyNames                 :
```

3. Inicie una operación de clonado de un grupo de recursos de clonado o un backup existente con el cmdlet New-SmClone.

   En este ejemplo, se crea un clon a partir de un determinado backup con todos los registros:

```
New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"}  -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

4. Puede consultar el estado del trabajo de clonado mediante el cmdlet Get-SmCloneReport.

   En este ejemplo, se muestra un informe de clonado con el correspondiente ID de trabajo:

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

## Supervisar las operaciones de clonado de recursos de plugins personalizados

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

**Acerca de esta tarea**

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Clonar**.
   d. En la lista desplegable **Estado**, seleccione el estado del clon.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

# Gestione SnapCenter Server y los plugins

## Consola de visualización

### Información general de la consola

En el panel de navegación de la izquierda de SnapCenter, Dashboard ofrece un primer vistazo sobre el estado del sistema, incluidas la actividad de trabajos recientes, las alertas, el resumen de la protección, la eficiencia y el uso del almacenamiento, el estado de los trabajos de SnapCenter (backup, clonado, restauración), el estado de configuración para los hosts independientes y de clústeres de Windows, Número de máquinas virtuales de almacenamiento (SVM) gestionadas por SnapCenter y capacidad de licencia.

La información que se muestra en la vista de consola varía según el rol asignado al usuario que ha iniciado sesión actualmente en SnapCenter. Es posible que no se muestre parte del contenido si el usuario no tiene permiso para ver dicha información.

En muchos casos, puede ver más información sobre una pantalla si pasa el ratón por **i**. En algunos casos, la información que se muestra en la consola está vinculada a información de origen detallada en páginas de la interfaz gráfica de usuario de SnapCenter, como Recursos, Monitor e informes.

#### Actividades laborales recientes

El icono Recent Job Activities muestra la actividad de trabajos más reciente en cualquier trabajo de backup, restauración y clonado al que tenga acceso. Los trabajos en esta pantalla tienen uno de los siguientes estados: Completed, Warning, Failed, Running, Queued, Y cancelada.

Pasar el ratón por encima de un trabajo proporciona más información. Puede ver información adicional del trabajo haciendo clic en un número de trabajo específico, que le redirige a la página Monitor. Desde ahí, puede obtener detalles del trabajo o información de registro, y generar un informe específico para ese trabajo.

Haga clic en **Ver todos** para ver un historial de todos los trabajos de SnapCenter.

#### Alertas

El icono Alertas muestra las alertas críticas y de advertencia más recientes sin resolver para los hosts y el servidor SnapCenter.

En la parte superior de la pantalla se muestra el número total de alertas críticas y de categoría Advertencia. Al hacer clic en los totales crítico o de advertencia, se le redirige a la página Alertas con el filtro específico aplicado en la página Alertas.

Al hacer clic en una alerta específica, se le redirigirá a la página Alertas para obtener más información sobre dicha alerta. Al hacer clic en **Ver todo** en la parte inferior de la pantalla, se le redirige a la página Alertas para ver una lista de todas las alertas.

#### Último resumen sobre protección

El icono Resumen de protección más reciente brinda el estado de protección de todas las entidades a las que se tiene acceso. De forma predeterminada, la pantalla se establece para proporcionar el estado de todos los

plugins. La información de estado se proporciona para los recursos cuyo backup se realiza en un almacenamiento primario como copias de Snapshot y en un almacenamiento secundario mediante tecnologías de SnapMirror y SnapVault. La información sobre el estado de protección para el almacenamiento secundario se basa en el tipo de plugin seleccionado.

Si utiliza una política de protección de reflejo-almacén, los contadores para el resumen de protección se muestran en el gráfico resumido SnapVault y no en el gráfico de SnapMirror.

El estado de protección para plugins individuales es disponible si selecciona un plugin en el menú desplegable. Un gráfico de donut muestra el porcentaje de recursos protegidos para el plugin seleccionado. Al hacer clic en un segmento de donut, se le redirige a la página **Informes** > **Plug-in**, que proporciona un informe detallado de toda la actividad de almacenamiento principal y secundario del plugin especificado.

Los informes sobre almacenamiento secundario se aplican solo a SnapVault; los informes de SnapMirror no se admiten.

SAP HANA proporciona información sobre el estado de protección para almacenamiento primario y secundario para copias de Snapshot. Solo el estado de protección del almacenamiento principal está disponible para backups basados en archivos.

| Estado de protección | Almacenamiento primario | Almacenamiento secundario |
|---|---|---|
| Error | Número de entidades que forman parte de un grupo de recursos, donde el grupo de recursos ha ejecutado un backup, pero ocurrió un error en el backup. | Número de entidades con backups que no se pudieron transferir a un destino secundario. |
| Exitoso | Número de entidades en un grupo de recursos, donde se realizó correctamente el backup del grupo de recursos. | Número de entidades con copias de seguridad que se transfirieron correctamente a un destino secundario. |
| No configurado | Número de entidades que no forman parte de ningún grupo de recursos y que no se han realizado backups. | Número de entidades que forman parte de uno o varios grupos de recursos que no se han configurado para que las copias de seguridad se transfieran a un destino secundario. |
| No iniciada | Número de entidades que forman parte de un grupo de recursos, pero no se ha ejecutado ningún backup. | No aplicable |

Si se utiliza SnapCenter Server 4.2 y una versión anterior del plugin (anterior a 4.2) para crear backups, el icono **Resumen de protección más reciente** no muestra el estado de protección de SnapMirror de estos backups.

### Trabajos

El icono Jobs brinda un resumen de los trabajos de backup, restauración y clonado a los que se puede acceder. Puede personalizar el lapso de tiempo para cualquier informe mediante el menú desplegable. Las opciones de lapso se corrigen en las últimas 24 horas, en los últimos 7 días y en los últimos 30 días. El informe predeterminado muestra los trabajos de protección de datos ejecutados en los últimos 7 días.

La información de trabajos de backup, restauración y clonado se muestra en los gráficos de donut. Al hacer clic en un segmento de donut, se le redirige a la página Monitor con filtros de trabajo previamente aplicados a la selección.

| Estado del trabajo | Descripción |
|---|---|
| Error | Número de trabajos que no se pudieron completar. |
| Advertencia | Número de trabajos en los que se produjo un error. |
| Exitoso | Número de trabajos completados correctamente. |
| Ejecutando | Recuento de trabajos que se están ejecutando actualmente. |

### Reducida

El icono almacenamiento muestra el almacenamiento primario y secundario que consumen los trabajos de protección en un periodo de 90 días, muestra gráficamente las tendencias de consumo y calcula el ahorro en almacenamiento primario. La información de almacenamiento se actualiza una vez cada 24 horas a las 12:00 a.m.

El total de consumo del día, que comprende el número total de backups disponibles en SnapCenter y el tamaño ocupado por estos backups, se mostrará en la parte superior de la pantalla. Un respaldo podría tener varias copias Snapshot asociadas y el número reflejará la misma. Esto se puede aplicar tanto a copias de Snapshot primarias como secundarias. Por ejemplo, ha creado 10 backups, de los cuales 2 se eliminan debido a la retención de backup basado en políticas y 1 backup se elimina explícitamente por usted. Por lo tanto, se mostrará el recuento de 7 backups junto con el tamaño ocupado por estos 7 backups.

El factor de ahorro en almacenamiento del almacenamiento primario es la proporción de la capacidad lógica (ahorros en copias Snapshot y clones, además del almacenamiento consumido) con la capacidad física del almacenamiento primario. Un gráfico de barras ilustra el ahorro en almacenamiento.

El gráfico de líneas traza por separado el consumo de almacenamiento primario y secundario día a día durante un período de 90 días rotativas. Pasar el puntero por los gráficos ofrece resultados detallados día a día.

> Si se utiliza SnapCenter Server 4.2 y una versión anterior del plugin (anterior a 4.2) para crear backups, el icono **almacenamiento** no muestra la cantidad de backups, el almacenamiento consumido por estos backups, el ahorro de Snapshot, el ahorro de clonado y el tamaño de la snapshot.

### Configuración

El icono Configuración proporciona información de estado consolidada para todos los hosts activos

independientes y de clústeres de Windows que SnapCenter gestiona, y a los que tiene acceso. Esto incluye la información de estado del plugin asociado con esos hosts.

Al hacer clic en el número adyacente a los hosts, se le redirige a la sección Managed hosts de la página hosts. Desde allí, es posible obtener información detallada de un host seleccionado.

Además, esta pantalla muestra la suma de las SVM independientes de ONTAP y de ONTAP de clúster que gestiona SnapCenter y a las que tiene acceso. Al hacer clic en el número adyacente a la SVM, se le redirigirá a la página sistemas de almacenamiento. A partir de ese punto, se puede obtener información detallada de una SVM seleccionada.

El estado de configuración del host se presenta como rojo (crítico), amarillo (advertencia) y verde (activo), junto con el número de hosts en cada estado. Los mensajes de estado se proporcionan para cada estado.

| Estado de configuración | Descripción |
|---|---|
| Actualización obligatoria | Número de hosts que ejecutan plugins no compatibles y necesitan una actualización. Esta versión de SnapCenter no admite un plugin no compatible. |
| Migración obligatoria | Número de hosts que ejecutan plugins no compatibles y necesitan migración. Esta versión de SnapCenter no admite un plugin no compatible. |
| No hay plugins instalados | El número de hosts que se añaden correctamente, pero es necesario instalar los plugins o se ha producido un error en la instalación de los plugins. |
| Suspendida | El número de hosts cuyas programaciones están suspendidas y están bajo mantenimiento. |
| Detenido | El número de hosts que están activos, pero los servicios de plugins no están en ejecución. |
| Host inactivo | Número de hosts inactivos o no accesibles. |
| Actualización disponible (opcional) | Cuente con los hosts en los que hay disponible una versión más reciente del paquete de plugins para su actualización. |
| Migración disponible (opcional) | Cuente con hosts en los que hay disponible una versión más reciente del plugin para la migración. |
| Configure el directorio de registro | Número de hosts donde debe configurarse el directorio de registro para que SCSQL realizar backup de registros de transacciones. |
| Configure los plugins de VMware | El número de hosts donde debe añadirse el plugin de SnapCenter para VMware vSphere. |

| Estado de configuración | Descripción |
|---|---|
| Desconocido | Número de hosts que se han registrado pero la instalación aún no se ha activado. |
| Ejecutando | El número de hosts que están activos y plugins en ejecución. Y en el caso de los plugins de SCSQL, se configuran el directorio de registro y el hipervisor. |
| Instalando\desinstalando plugins | Número de hosts en los que se está realizando la instalación o la desinstalación de plugins. |

**Capacidad con licencia**

El icono de capacidad con licencia muestra información sobre la capacidad total con licencia, la capacidad utilizada, las alertas de umbral de capacidad y las alertas de caducidad de licencias para licencias basadas en capacidad estándar de SnapCenter.

Esta pantalla solo aparece si se utilizan licencias basadas en capacidad estándar de SnapCenter en plataformas Cloud Volumes ONTAP o ONTAP Select. En el caso de las plataformas FAS o AFF, la licencia de SnapCenter se basa en controladoras y tiene licencias para ofrecer una capacidad ilimitada y no se necesita ninguna licencia por capacidad.

| Estado de la licencia | Descripción |
|---|---|
| En uso | Cantidad de capacidad actualmente en uso. |
| Notificar | Umbral de capacidad en el que se muestran notificaciones en la consola y, si se configuró esta opción, el momento en que se envían notificaciones. |
| Con licencia | Cantidad de capacidad que otorga la licencia. |
| Una vez | La cantidad de capacidad que ha superado la capacidad con licencia. |

## Cómo ver información en el panel

En el panel de navegación de la izquierda de SnapCenter, es posible ver varios iconos de la consola o mostrar, junto con los detalles del sistema asociados. El número de pantallas disponibles en el Panel es fijo y no se puede modificar. El contenido proporcionado en cada visualización depende del control de acceso basado en roles (RBAC).

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Panel**.
  2. Haga clic en las áreas activas de cada pantalla para obtener información adicional.

Por ejemplo, al hacer clic en un gráfico de donut en **Jobs**, le redirige a la página Monitor para obtener más información sobre su selección. Al hacer clic en un gráfico de donut en **Resumen de protección**, le redirige a la página Informes, que puede proporcionar más información sobre su selección.

## Solicite informes de estado de trabajos desde la consola

En la página Dashboard, es posible solicitar informes de trabajos de backup, restauración y clonado. Esto resulta útil para identificar la cantidad total de trabajos con errores o realizados correctamente en el entorno de SnapCenter.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Panel**
2. Busque el mosaico trabajos en el Panel y, a continuación, seleccione **copia de seguridad**, **Restaurar** o **Clonar**.
3. Con el menú desplegable, seleccione el lapso en que desea información de trabajo: 24 horas, 7 días o 30 días.

   Los sistemas muestran un gráfico de anillos que cubre los datos.

4. Haga clic en el corte de donut que representa la información del trabajo para la que desea obtener un informe.

   Al hacer clic en el gráfico de donut, se le redirigirá de la página Dashboard a la página Monitor. La página Monitor muestra los trabajos con el estado seleccionado en el gráfico de anillos.

5. En la lista de la página Monitor, haga clic en un trabajo específico para seleccionarlo.
6. En la parte superior de la página Monitor, haga clic en **Informes**.

**Resultados**

El informe muestra información solo sobre el trabajo seleccionado. Puede revisar el informe o descargarlo en su sistema local.

## Solicite informes sobre el estado de protección desde el panel de control

Es posible solicitar detalles de protección para los recursos gestionados por plugins específicos mediante la consola. Sólo se consideran los backups de datos para resumen de protección de datos.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Panel**.
2. Busque el icono Resumen de protección más reciente en la consola y utilice el menú desplegable para seleccionar un plugin.

   La consola muestra un gráfico de donut para los recursos que se han realizado backups en el almacenamiento principal y, si corresponde al plugin, un gráfico de donut para recursos respaldados en el almacenamiento secundario.

Los informes de protección de datos solo están disponibles para tipos de plugins específicos. No se admite la especificación de **todos los plugins**.

3. Haga clic en el corte de donut que representa el estado para el que desea obtener un informe.

   Al hacer clic en el gráfico de donut, se le redirigirá de la página Dashboard a Reports y, finalmente, a la página Plug-in. El informe muestra únicamente el estado del plugin seleccionado. Puede revisar el informe o descargarlo en su sistema local.

No se admite la redirección a la página Reports para el gráfico donut de SnapMirror y el backup de SAP HANA basado en archivos.

# Gestione RBAC

SnapCenter permite modificar roles, usuarios y grupos.

## Modificar un rol

Es posible modificar un rol de SnapCenter para quitar usuarios o grupos y cambiar los permisos asociados con el rol. Sobre todo es útil para modificar roles cuando se desean cambiar o eliminar los permisos usados por todo un rol.

**Lo que necesitará**

Inició sesión con el rol de administrador de SnapCenter.

No es posible modificar ni quitar permisos del rol de administrador de SnapCenter.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **roles**.
3. En el campo de nombre Role, haga clic en el rol que desea modificar.
4. En la página Role Details, modifique los permisos o anule la asignación de los miembros según sea necesario.
5. Seleccione **todos los miembros de esta función pueden ver los objetos de otros miembros** para permitir que otros miembros de la función vean recursos como volúmenes y hosts después de actualizar la lista de recursos.

   Anule la selección de esta opción si no desea que los miembros del rol vean los objetos a los que se asignaron otros miembros.

Cuando se habilita esta opción, no es necesario asignar a los usuarios acceso a los objetos o recursos si los usuarios pertenecen al mismo rol que el usuario que creó los objetos o recursos.

1. Haga clic en **Enviar**.

### Modificar usuarios y grupos

Es posible modificar usuarios o grupos de SnapCenter para modificar sus roles y activos.

**Lo que necesitará**

Debe iniciar sesión como administrador de SnapCenter.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **usuarios y acceso**.
  3. En la lista Nombre de usuario o de grupo, haga clic en el usuario o grupo que desea modificar.
  4. En la página de detalles Usuario o Grupo, modifique roles y activos.
  5. Haga clic en **Enviar**.

# Gestionar hosts

Es posible añadir hosts, instalar paquetes de plugins de SnapCenter, añadir un servidor de verificación, quitar hosts, migrar trabajos de backup y actualizar hosts para actualizar paquetes de plugins o añadir paquetes de plugins nuevos. Según el plugin que utilice, también puede aprovisionar discos, gestionar recursos compartidos SMB, gestionar grupos iniciadores (iGroups), gestionar sesiones iSCSI y migrar datos.

| Puede ejecutar estas tareas… | Para Microsoft Exchange Server | Para Microsoft SQL Server | Para Microsoft Windows | Para bases de datos de Oracle | Para base de datos SAP HANA | Para plugins personalizados |
|---|---|---|---|---|---|---|
| Añada los hosts e instale el paquete de plugins | Sí | Sí | Sí | Sí | Sí | Sí |
| Actualizar la información de ESXi para un host | No | Sí | No | No | No | No |
| Suspenda las programaciones y coloque los hosts en modo de mantenimiento | Sí | Sí | Sí | Sí | Sí | Sí |

| Puede ejecutar estas tareas… | Para Microsoft Exchange Server | Para Microsoft SQL Server | Para Microsoft Windows | Para bases de datos de Oracle | Para base de datos SAP HANA | Para plugins personalizados |
|---|---|---|---|---|---|---|
| Añadir, actualizar o quitar plugins para modificar hosts | Sí | Sí | Sí | Sí | Sí | Sí |
| Quite hosts de SnapCenter | Sí | Sí | Sí | Sí | Sí | Sí |
| Inicie servicios de plugin | Sí | Sí | Sí | Sí | Sí | Sí |
| Aprovisione los discos | No | No | Sí | No | No | No |
| Gestione los recursos compartidos de SMB | No | No | Sí | No | No | No |
| Gestionar los iGroups | No | No | Sí | No | No | No |
| Gestionar sesiones iSCSI | No | No | Sí | No | No | |

## Actualizar la información de la máquina virtual

Es conveniente actualizar la información de la máquina virtual cuando se reinicia el host del sistema de archivos o base de datos, se modifican las credenciales de VMware vCenter. Actualizar la información de la máquina virtual en SnapCenter inicia la comunicación con VMware vSphere vCenter y obtiene las credenciales de vCenter.

El plugin de SnapCenter para Microsoft Windows, que está instalado en el host de la base de datos, gestiona los discos basados en RDM. Para gestionar RDM, el plugin de SnapCenter para Microsoft Windows se comunica con el servidor de vCenter que gestiona el host de la base de datos.

- Pasos*
  1. En el panel de navegación izquierdo de SnapCenter, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.

3. En la página Managed hosts, seleccione el host que desea actualizar.
4. Haga clic en **Actualizar VM**.

## Modifique los hosts de plugins

Después de instalar un plugin, puede modificar los detalles de los hosts del plugin, si es preciso. Puede modificar las credenciales, la ruta de instalación, los plugins, los detalles del directorio de registro del plugin de SnapCenter para Microsoft SQL Server, la cuenta de servicio gestionada por los grupos (GMSA) y el puerto del plugin.

Asegúrese de que la versión del plugin sea la misma que la de la versión de SnapCenter Server.

**Acerca de esta tarea**

- Solo puede modificar un puerto de plugin después de instalar el plugin.

  No puede modificar el puerto del plugin mientras haya operaciones de actualización en curso.

- Al modificar el puerto de un plugin, debe tener en cuenta las siguientes posibles situaciones de reversión del puerto:
  - En una configuración independiente, si SnapCenter no logra cambiar el puerto de uno de los componentes, la operación genera un error y se conserva el puerto antiguo para todos los componentes.

    Si se ha cambiado el puerto para todos los componentes pero uno de los componentes sufre un error al arrancar con el puerto nuevo, se conserva el puerto antiguo para todos los componentes. Por ejemplo, si desea cambiar el puerto para dos plugins del host independiente y SnapCenter no logra aplicar el puerto nuevo a uno de los plugins, se produce un error en la operación (con el mensaje de error correspondiente) y se conserva el puerto antiguo para ambos plugins.

  - En una configuración de clúster, si SnapCenter no logra cambiar el puerto del plugin que está instalado en uno de los nodos, la operación genera un error y se conserva el puerto antiguo para todos los nodos.

    Por ejemplo, si el plugin se instala en cuatro nodos en una configuración de clúster y si el puerto no se cambia en uno de los nodos, se conserva el puerto antiguo para todos los nodos.

Cuando los plug-ins se instalan con GMSA, puede modificar en las ventanas de **más opciones**. Cuando los complementos se instalan sin GMSA, puede especificar la cuenta de GMSA para utilizarla como cuenta de servicio de complementos.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. Compruebe que **Managed hosts** está seleccionado en la parte superior.
  3. Seleccione el host para el que desea modificar y modificar cualquier campo.

     Sólo se puede modificar un campo a la vez.

  4. Haga clic en **Enviar**.

**Resultados**

El host se valida y agrega al servidor SnapCenter.

## Inicie o reinicie servicios de plugin

Al iniciar los servicios de plugins de SnapCenter, es posible iniciar servicios si no están en ejecución o reiniciarlos si ya lo están. Se recomienda reiniciar los servicios después de realizar tareas de mantenimiento.

Debe asegurarse de que no se están ejecutando trabajos al reiniciar los servicios.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. En la página Managed hosts, seleccione el host que desea iniciar.
  4. Haga clic en Y haga clic en **Iniciar servicio** o **Reiniciar servicio**.

     Puede iniciar o reiniciar el servicio de varios hosts al mismo tiempo.

## Suspender programaciones del mantenimiento del host

Si desea impedir que el host ejecute cualquier trabajo programado de SnapCenter, puede colocarlo en modo de mantenimiento. Debe hacerlo antes de actualizar los plugins o si va a realizar tareas de mantenimiento en los hosts.

No es posible suspender las programaciones en un host que está inactivo debido a que SnapCenter no se puede comunicar con ese host.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. En la página Managed hosts, seleccione el host que desea suspender.
  4. Haga clic en la Y, a continuación, haga clic en **Suspender programación** para colocar el host de este plugin en modo de mantenimiento.

     Puede suspender la programación de varios hosts al mismo tiempo.

     No es necesario detener el servicio de plugin primero. El servicio de plugin puede estar en un estado en ejecución o detenido.

**Resultados**

Después de suspender las programaciones en el host, la página Managed hosts muestra **suspendido** en el campo de estado general del host.

Después de completar el mantenimiento del host, puede sacar el host del modo de mantenimiento haciendo clic en **Activar programa**. Puede activar la programación de varios hosts al mismo tiempo.

# Operaciones admitidas en la página Resources

Es posible detectar recursos y realizar operaciones de protección de datos desde la página Resources. Las operaciones que puede realizar difieren en función del plugin que utiliza para gestionar sus recursos.

En la página Resources, es posible realizar las siguientes tareas:

| Puede ejecutar estas tareas… | Para Microsoft Exchange Server | Para Microsoft SQL Server | Para Microsoft Windows | Para bases de datos de Oracle | Para base de datos SAP HANA | Para plugins personalizados |
|---|---|---|---|---|---|---|
| Determine si hay recursos disponibles para backup | Sí | Sí | Sí | Sí | Sí | Sí |
| Llevar a cabo un backup bajo demanda de un recurso | Sí | Sí | Sí | Sí | Sí | Sí |
| Restaurar desde backups | Sí | Sí | Sí | Sí | Sí | Sí |
| Clonar backups | No | Sí | Sí | Sí | Sí | Sí |
| Gestionar backups | Sí | Sí | Sí | Sí | Sí | Sí |
| Gestionar clones | No | Sí | Sí | Sí | Sí | Sí |
| Gestionar políticas | Sí | Sí | Sí | Sí | Sí | Sí |
| Gestionar conexiones de almacenamiento | Sí | Sí | Sí | Sí | Sí | Sí |
| Montar backups | No | No | No | Sí | No | No |

| Puede ejecutar estas tareas… | Para Microsoft Exchange Server | Para Microsoft SQL Server | Para Microsoft Windows | Para bases de datos de Oracle | Para base de datos SAP HANA | Para plugins personalizados |
|---|---|---|---|---|---|---|
| Desmontar backups | No | No | No | Sí | No | No |
| Ver detalles | Sí | Sí | Sí | Sí | Sí | Sí |

# Gestionar políticas

Es posible desvincular políticas de un recurso o grupo de recursos, y modificar, eliminar, ver y copiar.

## Modificar políticas

Puede modificar las opciones de replicación, la configuración de retención de copias de Snapshot, el número de reintentos o la información de scripts mientras se asocia una política a un recurso o grupo de recursos. Puede modificar el tipo de programación (frecuencia) solo después de desvincular una política.

### Acerca de esta tarea

Para modificar el tipo de programación de una política se requieren otros pasos, ya que el servidor de SnapCenter registra el tipo de programación únicamente en el momento en que la política se vincula al recurso o al grupo de recursos.

| Si desea… | Realice lo siguiente… |
|---|---|
| Añada un tipo de programación adicional | Cree una nueva política y vincúlela a los recursos o grupos de recursos necesarios.<br><br>Por ejemplo, si la política de un grupo de recursos especifica solo backups por hora y usted también quiere añadir backups diarios, puede crear una política con un tipo de programación diaria y añadirla al grupo de recursos. El grupo de recursos tendrá, entonces, dos políticas de programación: Por hora y diaria. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Quite o cambie un tipo de programación | Realice lo siguiente:<br>1. Desvincule la política de cada recurso o grupo de recursos que use dicha política.<br>2. Modifique el tipo de programación.<br>3. Asocie la política otra vez a todos los recursos y grupos de recursos.<br>Por ejemplo, si una política especifica backups por hora y quiere cambiarla a backups diarios, primero debe desvincular la política. |

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Directivas**.
  3. Seleccione la directiva y, a continuación, haga clic en **Modificar**.
  4. Modifique la información y, a continuación, haga clic en **Finalizar**.

## Desvincular políticas

Es posible desvincular en cualquier momento políticas que ya no quiera que rijan la protección de datos de un recurso o de un grupo de recursos. Debe desvincular la política para poder eliminarla o para poder modificar el tipo de programación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Resource Group** en la lista **View**.
  3. Seleccione el grupo de recursos y, a continuación, haga clic en **Modificar grupo de recursos**.
  4. En la página Policies del asistente Modify Resource Group, en la lista desplegable, borre la selección junto a las políticas que desee desvincular.
  5. Haga las modificaciones adicionales que necesite el grupo de recursos en el resto del asistente y haga clic en **Finalizar**.

## Eliminar políticas

Si ya no se requieren políticas, es posible eliminarlas.

**Lo que necesitará**

Debe desvincular la política de los recursos o grupos de recursos si la política está asociada con cualquier recurso o grupo de recursos.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.

2. En la página Configuración, haga clic en **Directivas**.
3. Seleccione la directiva y, a continuación, haga clic en **Eliminar**.
4. Haga clic en **Sí**.

# Gestione grupos de recursos

Es posible realizar varias operaciones en grupos de recursos.

Es posible ejecutar las siguientes tareas relacionadas con los grupos de recursos:

- Modificar un grupo de recursos seleccionando el grupo de recursos y haciendo clic en **Modificar grupo de recursos** para editar la información suministrada al crear el grupo de recursos.

  Se puede cambiar la programación al modificar el grupo de recursos. Sin embargo, para cambiar el tipo de programación es necesario modificar la política.

  Si se quitan recursos de un grupo de recursos, la configuración de retención de backup definida en las políticas vinculadas al grupo de recursos seguirá aplicándose a los recursos quitados.

- Crear un backup de un grupo de recursos.
- Crear el clon de un backup.

  Puede clonar desde los backups existentes de SQL, Oracle, sistemas de archivos Windows, aplicaciones personalizadas y recursos de bases de datos SAP HANA o grupos de recursos.

- Crear el clon de un grupo de recursos.

  Esta operación solo es compatible para grupos de recursos SQL (que solo contienen bases de datos). Puede configurar una programación para clonar un grupo de recursos (ciclo de vida de clon).

- Impedir que se inicien operaciones programadas en grupos de recursos.
- Eliminar un grupo de recursos.

## Detenga y reanude operaciones en grupos de recursos

Es posible deshabilitar temporalmente el inicio de las operaciones programadas en un grupo de recursos. Más tarde, si se desea, se pueden habilitar las operaciones.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Resource Group** en la lista **View**.
  3. Seleccione el grupo de recursos y haga clic en **Mantenimiento**.
  4. Haga clic en **Aceptar**.

Si desea reanudar las operaciones en el grupo de recursos que ha puesto en modo de mantenimiento, seleccione el grupo de recursos y haga clic en **producción**.

## Eliminar grupos de recursos

Es posible eliminar un grupo de recursos si ya no es necesario proteger los recursos del grupo. Debe asegurarse de que los grupos de recursos se eliminen antes de poder quitar los plugins de SnapCenter.

**Acerca de esta tarea**

Debe eliminar manualmente todos los clones creados para los recursos del grupo de recursos. Otra opción es forzar la eliminación de todos los backups, los metadatos, las políticas y las copias de Snapshot que estén asociados con el grupo de recursos.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Resource Group** en la lista **View**.
  3. Seleccione el grupo de recursos y haga clic en **Eliminar**.
  4. Opcional: Marque la casilla de comprobación **Delete backups and detach policies associated with this Resource Group** para quitar todos los backups, los metadatos, las políticas y las copias de Snapshot que estén asociados con el grupo de recursos.
  5. Haga clic en **Aceptar**.

# Gestionar backups

Es posible cambiar el nombre de los backups y eliminarlos. También es posible eliminar varios backups simultáneamente.

## Cambiar el nombre de los backups

Es posible cambiar el nombre de los backups si se desea usar un nombre que facilite la búsqueda.

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
  3. Seleccione el recurso o el grupo de recursos de la lista.

     Se muestra la página con el resumen o grupo de recursos. Si el recurso o el grupo de recursos no está configurado para la protección de datos, se muestra el asistente Protect en lugar de la página Topology.

  4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principales.

     No puede cambiar el nombre de los backups que no están en el sistema de almacenamiento secundario.

  Si catalogó los backups de bases de datos de Oracle con Oracle Recovery Manager (RMAN), no puede cambiar el nombre de esos backups catalogados.

1. Seleccione el backup y, a continuación, haga clic en .
2. En el campo **Renombrar copia de seguridad como**, introduzca un nuevo nombre y haga clic en **Aceptar**.

## Eliminar backups

Es posible eliminar backups si ya no los requiere para otras operaciones de protección de datos.

**Lo que necesitará**

Debe haber eliminado los clones asociados antes de eliminar un backup.

Si un backup se asocia con un recurso clonado, ese backup no se puede eliminar.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
3. Seleccione el recurso o el grupo de recursos de la lista.

   Se muestra la página con el resumen o grupo de recursos.

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principales.

   No puede eliminar los backups que están en el sistema de almacenamiento secundario.

5. Seleccione el backup y, a continuación, haga clic en .

   Si va a eliminar un backup de base de datos SAP HANA, los catálogos SAP HANA asociados del backup también se eliminan.

Si se elimina el último backup restante, no se pueden eliminar las entradas del catálogo HANA asociadas.

1. Haga clic en **Aceptar**.

Si tiene algunos backups obsoletos de bases de datos en SnapCenter que no corresponden a ningún backup en el sistema de almacenamiento, debe emplear el comando remove-smbackup para borrar dichas entradas de backup obsoletos. Si se catalogaron los backups obsoletos, se descatalogarán de la base de datos del catálogo de recuperación.

# Eliminar clones

Puede eliminar clones si ya no le resultan necesarios.

**Acerca de esta tarea**

No puede eliminar clones que actúan como origen para otros clones.

Por ejemplo, si la base de datos de producción es db1, el clon 1 de la base de datos se clona desde el backup de db1 y, después, se protege el clon 1. La base de datos que clona el clon 2 se clona a partir del backup del clon 1. Si decide eliminar el clon 1, primero debe eliminar el clon 2 y luego eliminar el clon 1.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
  3. Seleccione el recurso o el grupo de recursos de la lista.

     Se muestra la página con el resumen o grupo de recursos.
  4. En la vista Manage Copies (Administrar copias), seleccione **Clones** ya sea en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
  5. Seleccione el clon y, a continuación, haga clic en .

     Si elimina clones de bases de datos SAP HANA, en la página Delete Clone, lleve a cabo las acciones siguientes:

     a. En el campo **Pre clone delete**, introduzca los comandos que se deben ejecutar antes de eliminar el clon.
     b. En el campo **Unmount**, introduzca el comando para desmontar el clon antes de eliminarlo.
  6. Haga clic en **Aceptar**.

**Después de terminar**

A veces los sistemas de archivos no se eliminan. Debe aumentar el valor del parámetro CLONE_DELETE_DELAY ejecutando el siguiente comando: `./sccli Set-SmConfigSettings`

> El parámetro CLONE_DELETE_DELAY especifica la cantidad de segundos que debe esperarse luego de completar la eliminación del clon de la aplicación para comenzar la eliminación del sistema de archivos.

Después de modificar el valor del parámetro, reinicie SnapCenter el servicio del SPL.

# Supervisar trabajos, programaciones, eventos y registros

Es posible supervisar el progreso de los trabajos, obtener información sobre los trabajos programados, y revisar eventos y registros en la página Monitor.

## Supervisar trabajos

Es posible ver información de los trabajos de backup, clonado, restauración y verificación de SnapCenter. Puede filtrar esta vista en función de la fecha de inicio y de finalización, el tipo de trabajo, el grupo de recursos, la política o el plugin de SnapCenter. También se pueden obtener más detalles y archivos de registro de los trabajos especificados.

Asimismo, es posible supervisar los trabajos relacionados con operaciones de SnapMirror y SnapVault.

Puede supervisar únicamente los trabajos que creó y que son relevantes para su caso, a menos que tenga asignado el rol de administrador de SnapCenter u otro rol de superusuario.

Puede ejecutar las siguientes tareas relacionadas con los trabajos de supervisión:

- Supervisar las operaciones de backup, clonado, restauración y verificación.
- Ver detalles del trabajo e informes.
- Detener un trabajo programado.

## Supervisar programaciones

Es posible ver las programaciones actuales para determinar cuándo se iniciará la operación, cuándo se ejecutó por última vez y cuándo será la próxima ejecución. También se puede determinar el host donde se ejecutará la operación, junto con la información de la política y el grupo de recursos de la operación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Monitor, haga clic en **programas**.
  3. Seleccione el grupo de recursos y el tipo de programación.
  4. Consulte la lista de operaciones programadas.

## Supervisar eventos

Es posible ver una lista de eventos de SnapCenter en el sistema, como cuando un usuario crea un grupo de recursos o cuando el sistema inicia actividades, por ejemplo, la creación de un backup programado. Los eventos pueden verse para determinar si una operación de backup o restauración está actualmente en curso.

### Acerca de esta tarea

Toda la información sobre eventos se muestra en la página Events. Por ejemplo, cuando se inicia una tarea de copia de seguridad, aparece el evento «'backup start'». Cuando finalice el backup, se mostrará el evento «'backup completado».

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Monitor, haga clic en **Eventos**.
  3. (Opcional) en el cuadro filtro, introduzca la fecha de inicio o finalización, la categoría del evento (copia de seguridad, grupo de recursos o política) y el nivel de gravedad, y haga clic en **aplicar**. Otra opción es escribir los caracteres en el recuadro Search.
  4. Consulte la lista de eventos.

## Supervisar registros

Es posible ver y descargar registros del servidor de SnapCenter, registros del agente de host de SnapCenter y registros de plugins. Los registros pueden verse para facilitar la solución de problemas.

### Acerca de esta tarea

Puede filtrar los registros para mostrar solamente un nivel de gravedad de un registro específico:

- Depurar
- Información
- Advertir
- Error
- Fatal

También puede obtener los registros del nivel del trabajo, por ejemplo, los registros que permiten resolver el motivo del error de un trabajo de backup. Para los registros de nivel de trabajo, utilice la opción **Monitor** > **trabajos**.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Jobs, seleccione un trabajo y haga clic en Download logs.

     La carpeta comprimida descargada contiene los registros de trabajos y los registros comunes. El nombre de la carpeta comprimida contiene el ID de trabajo y el tipo de trabajo seleccionados.
  3. En la página Monitor, haga clic en **Logs**.
  4. Seleccione el tipo de registro y la instancia.

     Si selecciona el tipo de registro como **plugin**, puede seleccionar un host o un complemento SnapCenter. No puede hacer esto si el tipo de registro es **Server**.
  5. Para filtrar los registros por un origen, mensaje o nivel de registro en particular, haga clic en el icono de filtro ubicado arriba del título de la columna.

     Para mostrar todos los registros, seleccione **mayor o igual a** como `Debug` nivel.
  6. Haga clic en **Actualizar**.
  7. Consulte la lista de registros.
  8. Haga clic en **Descargar** para descargar los registros.

     La carpeta comprimida descargada contiene los registros de trabajos y los registros comunes. El nombre de la carpeta comprimida contiene el ID de trabajo y el tipo de trabajo seleccionados.

En configuraciones de gran tamaño para un rendimiento óptimo, debe establecer la configuración del registro para SnapCenter en el nivel mínimo mediante el cmdlet de PowerShell.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

Para acceder a la información de estado o de configuración después de que finalice un trabajo de conmutación por error, ejecute el cmdlet `Get-SmRepositoryConfig`.

## Quite los trabajos y los registros de SnapCenter

Es posible quitar registros y trabajos de backup, restauración, clonado y verificación de SnapCenter. SnapCenter almacena los registros de los trabajos con errores y aquellos completados correctamente a menos que se los elimine. Puede quitarlos para reaprovisionar el almacenamiento.

**Acerca de esta tarea**

No debe haber trabajos actualmente en ejecución. Puede quitar un trabajo específico si proporciona un identificador del trabajo, o bien puede eliminar los trabajos dentro de un periodo determinado.

No es necesario poner el host en modo de mantenimiento para quitar un trabajo.

- Pasos*
  1. Inicie PowerShell.
  2. En el símbolo del sistema, introduzca: `Open-SMConnection`
  3. En el símbolo del sistema, introduzca: `Remove-SmJobs`
  4. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  5. En la página Monitor, haga clic en **Jobs**.
  6. En la página Jobs, revise el estado del trabajo.

**Más información**

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

# Información general sobre las funcionalidades de generación de informes de SnapCenter

SnapCenter ofrece distintas opciones de generación de informes que permiten supervisar y gestionar el estado y el éxito operativo del sistema.

| Tipo de informe | Descripción |
|---|---|
| Informe de copia de seguridad | Backup Report ofrece datos generales sobre las tendencias de backup en el entorno de SnapCenter, la tasa de éxito de backups y detalles sobre cada uno de los backups realizados durante el periodo específico. Si se elimina un backup, el informe no muestra ninguna información de estado del backup eliminado. Backup Detail Report ofrece información detallada sobre un trabajo de backup especificado y muestra los recursos respaldados correctamente, además de todos los que generaron errores. |

| Tipo de informe | Descripción |
| --- | --- |
| Clonar informe | Clone Report ofrece datos generales sobre las tendencias de clonado en el entorno de SnapCenter, la tasa de éxito de clones y detalles sobre cada uno de los clones realizados durante el periodo específico. Si se elimina un clon, el informe no muestra ninguna información de estado del clon eliminado. Clone Detail Report ofrece detalles sobre el estado de la tarea de clonado, el host del clon y el trabajo de clonado especificados. Si no se puede completar una tarea, Clone Detail Report muestra información sobre el error. |
| Restaurar informe | Restore Report ofrece información general sobre los trabajos de restauración. Restore Detail Report ofrece detalles sobre un trabajo de restauración específico, incluidos el nombre de host, el nombre de backup, el inicio y la duración del trabajo, y el estado de las tareas de trabajos individuales. Si no se puede completar una tarea, Restore Detail Report muestra información sobre el error. |
| Informe de protección | Estos informes ofrecen detalles de protección para los recursos gestionados por todas las instancias del plugin de SnapCenter. Este informe ofrece detalles de protección para los recursos gestionados por todas las instancias del plugin. Puede ver información general, detalles de recursos no protegidos, recursos que no se han realizado backups cuando se genera el informe, recursos de un grupo de recursos para el cual las operaciones de backup han generado errores, y el estado de SnapVault. |

| Tipo de informe | Descripción |
| --- | --- |
| Informe programado | Estos informes se programan para que se ejecuten periódicamente, como diariamente, semanalmente o mensualmente. Los informes se generan automáticamente en la fecha y hora especificadas y el informe se envía a las respectivas personas por correo electrónico Es posible habilitar, deshabilitar, modificar o eliminar las programaciones. La programación activada se puede ejecutar a petición haciendo clic en el botón **Ejecutar ahora**. El administrador puede ejecutar cualquier programación, pero el informe generado contendrá datos basados en el permiso proporcionado por el usuario que creó la programación.<br><br>Cualquier otro usuario que no sea el Administrador podrá ver o modificar la planificación según su permiso. Si todos los miembros de esta función pueden ver los objetos de otros miembros están seleccionados en la página Agregar función, otros miembros de la función podrán ver y modificar. |

## Acceder a informes

Puede usar la consola de SnapCenter para obtener una descripción rápida del estado del sistema. Desde la consola, podrá obtener información detallada. También puede acceder a los informes detallados directamente.

Puede acceder a los informes mediante uno de los siguientes métodos:

- En el panel de navegación izquierdo, haga clic en **Panel** y, a continuación, haga clic en el gráfico circular **último resumen de protección** para ver más detalles en la página Informes.
- En el panel de navegación de la izquierda, haga clic en **Informes**.

## Filtre su informe

Se recomienda filtrar los datos del informe de acuerdo con un rango de parámetros, según el nivel de detalles y el intervalo de tiempo de la información que se necesita.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Informes**.
  2. Si no se muestra la vista Parameter, haga clic en el icono **Toggle Parameters Area** en la barra de herramientas de informes.
  3. Especifique el rango de tiempo sobre el que desea ejecutar el informe. + Si omite la fecha de finalización, recuperará toda la información disponible.
  4. Filtre la información de los informes en función de alguno de los siguientes criterios:
     - Grupo de recursos
     - Host
     - Política

- Recurso
- Estado
- Nombre de complemento

5. Haga clic en **aplicar**.

## Exportar o imprimir informes

La exportación de los informes de SnapCenter permite ver los informes en diversos formatos alternativos. También es posible imprimir los informes.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Informes**.
  2. Desde la barra de herramientas de informes, realice una de las siguientes acciones:
     - Haga clic en el icono **Toggle Print Preview** para obtener una vista previa de un informe imprimible.
     - Seleccione un formato de la lista desplegable del icono **Exportar** para exportar un informe a un formato alternativo.
  3. Para imprimir un informe, haga clic en el icono **Imprimir**.
  4. Para ver un resumen de un informe específico, desplácese a la sección apropiada del informe.

## Establezca el servidor SMTP para las notificaciones por correo electrónico

Es posible especificar el servidor SMTP que se utilizará para enviar informes de trabajos de protección de datos a usted mismo o a terceros. También es posible enviar un mensaje de correo electrónico para comprobar la configuración. Los ajustes se aplican globalmente en cualquier trabajo de SnapCenter para el que configure las notificaciones por correo electrónico.

Esta opción configura el servidor SMTP para enviar todos los informes de trabajos de protección de datos. Sin embargo, si desea enviar actualizaciones de trabajos de protección de datos de SnapCenter regulares relacionadas con un recurso particular a usted mismo o a terceros, para poder supervisar esas actualizaciones, puede configurar la opción para enviar por correo electrónico los informes de SnapCenter cuando crea un grupo de recursos.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Configuración global**.
  3. Introduzca el servidor SMTP y haga clic en **Guardar**.
  4. Para enviar un mensaje de correo electrónico de prueba, introduzca la dirección de correo electrónico desde y hacia la que enviará el mensaje, introduzca el asunto y haga clic en **Enviar**.

## Configure la opción para enviar informes por correo electrónico

Si desea enviar actualizaciones de trabajos de protección de datos de SnapCenter regulares a usted mismo o a terceros para poder supervisar esas actualizaciones, puede configurar la opción para enviar por correo electrónico los informes de SnapCenter cuando crea un grupo de recursos.

**Lo que necesitará**

Configuró el servidor SMTP en la página Global Settings, en Settings.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Seleccione el tipo de recurso que desea ver y haga clic en **Nuevo grupo de recursos**, o seleccione un grupo de recursos existente y haga clic en **Modificar** para configurar informes por correo electrónico para un grupo de recursos existente.
  3. En el panel Notification del asistente New Resource Group, seleccione en las opciones del menú desplegable si desea recibir informes siempre, en caso de error, o en caso de error o advertencia.
  4. Introduzca la dirección del remitente, la dirección del destinatario y el asunto del correo electrónico.

# Gestione el repositorio del servidor SnapCenter

La información relacionada con las diversas operaciones que se ejecutan en SnapCenter se almacena en el repositorio de base de datos de servidor de SnapCenter. Es necesario crear backups del repositorio para proteger al servidor SnapCenter de una pérdida de datos.

El repositorio del servidor SnapCenter se denomina a veces base de datos NSM.

## Requisitos previos para proteger el repositorio de SnapCenter

El entorno debe cumplir con ciertos requisitos previos para proteger el repositorio de SnapCenter.

- Gestionar conexiones de SVM

  Debe configurar las credenciales de almacenamiento.

- Aprovisionar hosts

  Debe haber al menos un disco de almacenamiento de NetApp en el host de repositorio de SnapCenter. Si no hay un disco de NetApp en el host de repositorio de SnapCenter, debe crearlo.

  Para obtener detalles sobre cómo añadir hosts, configurar conexiones de SVM y aprovisionar hosts, consulte las instrucciones de instalación.

- Aprovisionar LUN de iSCSI o VMDK

  Para la configuración de alta disponibilidad, puede aprovisionar un LUN de iSCSI o un VMDK en uno de los servidores SnapCenter.

## Realice un backup del repositorio de SnapCenter

Realizar un backup del repositorio de servidor de SnapCenter permite protegerlo contra la pérdida de datos. Para realizar un backup del repositorio, es necesario ejecutar el cmdlet *Protect-SmRepository*.

**Acerca de esta tarea**

El cmdlet *Protect-SmRepository* realiza las siguientes tareas:

- Crea un grupo de recursos y una política
- Crea una programación de backups para el repositorio de SnapCenter
- Pasos*
  1. Inicie PowerShell.
  2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet _Open-SmConnection y, a continuación, introduzca sus credenciales.
  3. Realice un backup del repositorio con el cmdlet *Protect-SmRepository* y los parámetros necesarios.

## Ver los backups del repositorio de SnapCenter

Para ver una lista de backups del repositorio de base de datos de SnapCenter Server, es posible ejecutar el cmdlet *Get-SmRepositoryBackups*.

Los backups del repositorio se crean según la programación especificada en el cmdlet *Protect-SmRepository*.

- Pasos*
  1. Inicie PowerShell.
  2. En el símbolo del sistema, introduzca el cmdlet siguiente y, a continuación, proporcione credenciales para conectarse al servidor SnapCenter: *Open-SMConnection*
  3. Obtenga una lista de todos los backups de base de datos de SnapCenter disponibles con el cmdlet *Get-SmRepositoryBackups*.

## Restaurar el repositorio de la base de datos de SnapCenter

Para restaurar el repositorio de SnapCenter, es posible ejecutar el cmdlet *Restore-SmRepositoryBackup*.

Cuando se restaura el repositorio de SnapCenter, se verán afectadas otras operaciones de SnapCenter que se estén ejecutando debido a que no se puede acceder a la base de datos del repositorio durante la operación de restauración.

- Pasos*
  1. Inicie PowerShell.
  2. En el símbolo del sistema, introduzca el cmdlet siguiente y, a continuación, proporcione credenciales para conectarse al servidor SnapCenter: *Open-SMConnection*
  3. Restaure el backup del repositorio con el cmdlet *Restore-SmRepositoryBackup*.

     El siguiente cmdlet restaura el repositorio de bases de datos MySQL de SnapCenter desde los backups que existen en el LUN de iSCSI o VMDK:

     ```
     C:\PS>Restore-SmRepositoryBackup -BackupName
     MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
     ```

     El siguiente cmdlet restaura la base de datos MySQL de SnapCenter cuando se eliminan accidentalmente los archivos de backup del LUN de iSCSI. Para VMDK, restaure manualmente desde copias de Snapshot de ONTAP.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

## Migre el repositorio de SnapCenter

Es posible migrar el repositorio de la base de datos del servidor de SnapCenter de la ubicación predeterminada a otro disco. El repositorio puede migrarse cuando se desea reubicarlo en un disco con más espacio.

- Pasos*
  1. Detenga el servicio MYSQL57 en Windows.
  2. Ubique el directorio de datos de MySQL.

     Normalmente, puede encontrar el directorio de datos en C:\ProgramData\MySQL\MySQL Server 5.7\Data.
  3. Copie el directorio de datos de MySQL en la nueva ubicación, por ejemplo, E:\Data\nsm.
  4. Haga clic con el botón derecho en el nuevo directorio y seleccione **Propiedades** > **Seguridad** para agregar la cuenta de servidor local de Network Service al nuevo directorio y, a continuación, asigne el control total de la cuenta.
  5. Cambie el nombre del directorio original de la base de datos, por ejemplo, nsm_copy.
  6. Desde un símbolo del sistema de Windows, cree un vínculo de directorio simbólico mediante el comando *mklink*.

     ```
     "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
     ```
  7. Inicie el servicio MYSQL57 en Windows.
  8. Compruebe que la ubicación de la base de datos se haya modificado correctamente; para ello, inicie sesión en SnapCenter y verifique las entradas del repositorio, o inicie sesión en la utilidad MySQL y conéctese al nuevo repositorio.
  9. Elimine el directorio original del repositorio de la base de datos al que cambió el nombre (nsm_copy).

## Restablecer la contraseña del repositorio de SnapCenter

La contraseña de la base de datos del repositorio del servidor MySQL se genera automáticamente durante la instalación del servidor SnapCenter desde SnapCenter 4.2. El usuario de SnapCenter no conoce esta contraseña generada automáticamente en ningún momento. Si se desea acceder a la base de datos del repositorio, se debe restablecer la contraseña.

**Lo que necesitará**

Debe tener los privilegios de administrador de SnapCenter para restablecer la contraseña.

- Pasos*
  1. Inicie PowerShell.
  2. En el símbolo del sistema, introduzca el siguiente comando y, a continuación, proporcione las credenciales para conectarse al servidor SnapCenter: *Open-SMConnection*

3. Restablezca la contraseña del repositorio: *Set-SmRepositoryPassword*

   El siguiente comando restablece la contraseña de repositorio:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

**Más información**

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

# Gestione recursos de dominios que no son de confianza

Además de gestionar hosts en dominios de confianza de Active Directory (AD), SnapCenter también gestiona hosts en varios dominios de AD que no son de confianza. Los dominios AD que no son de confianza deben registrarse en el servidor SnapCenter. SnapCenter admite usuarios y grupos de varios dominios AD que no son de confianza.

Puede instalar el servidor SnapCenter en un equipo que esté en un dominio o grupo de trabajo. Para instalar SnapCenter Server, debe especificar las credenciales de dominio si el equipo está en un dominio o las credenciales de administrador local si el equipo está en un grupo de trabajo.

No se admiten los grupos de Active Directory (AD) que pertenecen a dominios no registrados en el servidor de SnapCenter. Aunque es posible crear roles de SnapCenter con estos grupos de AD, se produce un error al iniciar sesión en SnapCenter Server con el siguiente mensaje de error: El usuario que intenta iniciar sesión no pertenece a ningún rol. Póngase en contacto con el administrador.

## Modificar dominios que no son de confianza

Puede modificar un dominio que no es de confianza cuando desea actualizar las direcciones IP del controlador de dominio o el nombre de dominio completo (FQDN).

**Acerca de esta tarea**

Después de modificar el FQDN, los activos asociados (hosts, usuarios y grupos) pueden no funcionar como se espera.

Para modificar un dominio que no es de confianza, puede utilizar la interfaz de usuario de SnapCenter o cmdlets de PowerShell.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Configuración global**.

3. En la página Global Settings (Configuración global), haga clic en **Configuración de dominio**.
4. Haga clic en y, a continuación, proporcione los siguientes detalles:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Dominio FQDN | Especifique el FQDN y haga clic en **resolver**. |
| Direcciones IP del controlador de dominio | Si el dominio FQDN no es resoluble, especifique una o más direcciones IP de controlador de dominio. |

5. Haga clic en **Aceptar**.

### Cancele el registro de dominios de Active Directory que no son de confianza

Puede cancelar el registro de un dominio de Active Directory que no sea de confianza si no desea utilizar los activos asociados a ese dominio.

**Lo que necesitará**

Debe haber quitado los hosts, los usuarios, los grupos y las credenciales que están asociados con el dominio de no confianza.

**Acerca de esta tarea**

- Una vez que se cancela el registro del dominio en el servidor SnapCenter, los usuarios de ese dominio no pueden tener acceso a SnapCenter Server.
- Si existen activos asociados (hosts, usuarios y grupos), después de cancelar el registro del dominio, los activos no estarán operativos.
- Para cancelar el registro de un dominio que no es de confianza, puede utilizar la interfaz de usuario de SnapCenter o cmdlets de PowerShell.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Configuración global**.
  3. En la página Global Settings (Configuración global), haga clic en **Configuración de dominio**.
  4. En la lista de dominios, seleccione el dominio al que desea cancelar el registro.
  5. Haga clic en Y, a continuación, haga clic en **Aceptar**.

# Gestione el sistema de almacenamiento

Después de añadir el sistema de almacenamiento, es posible modificar las conexiones y la configuración del sistema de almacenamiento, o eliminar el sistema de almacenamiento.

## Modifique la configuración del sistema de almacenamiento

Puede usar SnapCenter para modificar la configuración del sistema de almacenamiento si desea cambiar el nombre de usuario, la contraseña, la plataforma, el puerto, el protocolo, Período de tiempo de espera, dirección IP preferida o opciones de mensajería.

**Acerca de esta tarea**

Es posible modificar las conexiones de almacenamiento para un usuario individual o un grupo. Si pertenece a uno o varios grupos con permiso al mismo sistema de almacenamiento, el nombre de la conexión de almacenamiento se muestra varias veces en la lista de conexiones de almacenamiento, una vez para cada grupo con permiso al sistema de almacenamiento.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **sistemas de almacenamiento**.
  2. En la página Storage Systems, en el menú desplegable **Tipo**, realice una de las siguientes acciones:

| Seleccione… | Pasos… |
| --- | --- |
| SVM de ONTAP | Ver todas las máquinas virtuales de almacenamiento (SVM) que se añadieron y modificar la configuración de SVM necesaria.<br><br>a. En la página Storage Connections, haga clic en el nombre SVM adecuado.<br>b. Ejecute una de las siguientes acciones:<br><br>◦ Si la SVM no forma parte de ningún clúster, en la página Modify Storage System, modifique las configuraciones como el nombre de usuario, la contraseña, la configuración de EMS y AutoSupport, la plataforma, el protocolo, el puerto, el tiempo de espera, Y la IP preferida.<br>◦ Si el SVM forma parte de un clúster, en la página Modify Storage System, seleccione * Manage SVM independientemente* y modifique las configuraciones como el nombre de usuario, la contraseña, la configuración de EMS y AutoSupport, la plataforma, el protocolo, el puerto, el tiempo de espera, Y la IP preferida.<br><br>Después de modificar la SVM para que se gestione de forma independiente, si decide gestionarla a través del clúster, debe eliminar la SVM y, a continuación, hacer clic en **Rediscover**. La SVM se añadirá al clúster de ONTAP.<br><br>Cuando se actualiza una contraseña del sistema de almacenamiento en la interfaz gráfica de usuario de SnapCenter, es necesario reiniciar los servicios de SMCore del plugin correspondiente o el host de servidor debido a que la contraseña actualizada no aparece en SMCore y los trabajos de backup fallarán con un error de credencial incorrecto. |

| Seleccione… | Pasos… |
| --- | --- |
| Clústeres ONTAP | Para ver todos los clústeres que se han añadido y modificar la configuración de clúster necesaria.<br>a. En la página Storage Connections, haga clic en el nombre del clúster.<br>b. En la página Modify Storage System, haga clic en el icono para editar al lado de Username y modifique el nombre de usuario y la contraseña.<br>c. Seleccione o borre la configuración de EMS y AutoSupport.<br>d. Haga clic en **más opciones** y modifique otras configuraciones como la plataforma, el protocolo, el puerto, el tiempo de espera y la IP preferida. |

3. Haga clic en **Enviar**.

## Elimine el sistema de almacenamiento

Se puede usar SnapCenter para eliminar el sistema de almacenamiento que no se utiliza.

**Acerca de esta tarea**

Es posible eliminar conexiones de almacenamiento para un usuario individual o un grupo. Si pertenece a uno o varios grupos con permiso al mismo sistema de almacenamiento, el nombre del sistema de almacenamiento se muestra varias veces en la lista de conexiones de almacenamiento, una vez para cada grupo con permiso al sistema de almacenamiento.

Cuando se elimina un sistema de almacenamiento, se producirá un error en todas las operaciones que se están realizando en ese sistema de almacenamiento.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **sistemas de almacenamiento**.
2. En la página sistemas de almacenamiento, en el menú desplegable **Tipo**, seleccione **ONTAP SVM** o **clústeres ONTAP**.
3. En la página Storage Connections, seleccione la casilla de comprobación junto a SVM o el clúster que desea eliminar.

   No puede seleccionar la SVM que forma parte de un clúster.

4. Haga clic en **Eliminar**.
5. En la página Delete Storage System Connection Settings (Eliminar configuración de conexión del sistema de almacenamiento), haga clic en **OK**.

Si se elimina una SVM del clúster de ONTAP mediante la interfaz gráfica de usuario de ONTAP, en la interfaz gráfica de usuario de SnapCenter, haga clic en **Rediscover** para actualizar la lista de SVM.

# Gestione la recogida de datos de EMS

Es posible programar y gestionar la recogida de datos de Event Management System (EMS) mediante cmdlets de PowerShell. La recogida de datos de EMS implica recopilar datos sobre SnapCenter Server, los paquetes de plugins de SnapCenter instalados, los hosts y datos similares y, posteriormente, enviarlos a una máquina virtual de almacenamiento (SVM) específica de ONTAP.

La utilización de la CPU del sistema es alta cuando la tarea de recopilación de datos está en curso. El uso de la CPU sigue siendo elevado siempre que la operación se haga avanzar con independencia del tamaño de los datos.

## Detenga la recogida de datos de EMS

La recogida de datos de EMS se encuentra habilitada de forma predeterminada, y se ejecuta cada siete días después de la fecha de instalación. Es posible deshabilitar la recogida de datos en cualquier momento con el cmdlet de PowerShell *Disable-SmDataCollectionEMS*.

- Pasos*
  1. Desde una línea de comandos de PowerShell, establezca una sesión con SnapCenter introduciendo *Open-SmConnection*.
  2. Deshabilite la recogida de datos de EMS. Para ello, introduzca *Disable-SmDataCollectionEms*.

## Inicie la recogida de datos de EMS

De forma predeterminada, la recogida de datos de EMS se encuentra habilitada y programada para ejecutarse cada siete días desde la fecha de instalación. Si la deshabilitó, puede iniciar nuevamente la recogida de datos de EMS con el cmdlet *Enable-SmDataCollectionEMS*.

Se otorgó el permiso event generate-autosupport-log de Data ONTAP al usuario de la máquina virtual de almacenamiento (SVM).

- Pasos*
  1. Desde una línea de comandos de PowerShell, establezca una sesión con SnapCenter introduciendo *Open-SmConnection*.
  2. Habilite la recogida de datos de EMS. Para ello, introduzca *Enable-SmDataCollectionEMS*.

## Cambie la programación de recogida de datos de EMS y SVM de destino

Es posible utilizar cmdlets de PowerShell para cambiar la programación de recogida de datos de EMS o las máquinas virtuales de almacenamiento (SVM) de destino.

- Pasos*
  1. Desde una línea de comandos de PowerShell, para establecer una sesión con SnapCenter, introduzca

el cmdlet *Open-SmConnection*.

2. Para cambiar el destino de recogida de datos de EMS, introduzca el cmdlet *Set-SmDataCollectionEmsTarget*.
3. Para cambiar la programación de recogida de datos de EMS, introduzca el cmdlet *Set-SmDataCollectionEmsSchedule*.

## Supervise el estado de recogida de datos de EMS

Es posible supervisar el estado de la recogida de datos de EMS mediante varios cmdlets de PowerShell. Se puede obtener información sobre la programación, la SVM, el destino y el estado.

- Pasos*
  1. Desde una línea de comandos de PowerShell, establezca una sesión con SnapCenter introduciendo *Open-SmConnection*.
  2. Recupere información sobre la programación de recogida de datos de EMS. Para ello, introduzca *Get-SmDataCollectionEmsSchedule*.
  3. Recupere información sobre el estado de la recogida de datos de EMS. Para ello, introduzca *Get-SmDataCollectionEmsStatus*.
  4. Recupere información acerca del destino de recogida de datos de EMS. Para ello, introduzca *Get-SmDataCollectionEmsTarget*.

### Más información

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

# Actualice el servidor de SnapCenter y los plugins

## Configure SnapCenter para la búsqueda de actualizaciones disponibles

SnapCenter se comunica de forma periódica con el sitio de soporte de NetApp para notificar acerca de las actualizaciones de software disponibles. También puede crear una programación para especificar el intervalo en el que desea recibir información acerca de las actualizaciones disponibles.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Software**.

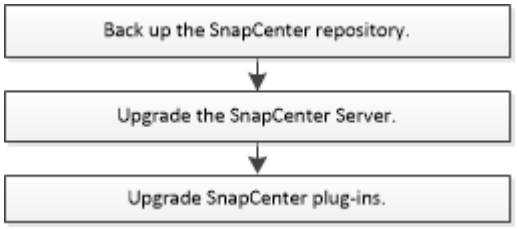
     La página Available Software muestra los paquetes de plugins y las versiones disponibles, así como su estado de instalación.

  3. Haga clic en **Buscar actualizaciones** para ver si hay alguna versión más reciente de los paquetes de complementos disponibles.
  4. Haga clic en **programar actualizaciones** para crear un programa que especifique el intervalo en el que desea recibir información acerca de las actualizaciones disponibles:
     a. Seleccione el intervalo en **Buscar actualizaciones**.
     b. Seleccione la credencial de administración de servidor SnapCenter para Windows y haga clic en **Aceptar**.

## Actualizar el flujo de trabajo

Cada versión de SnapCenter contiene un servidor SnapCenter y un paquete de plugins actualizados. Las actualizaciones del paquete de plugins se distribuyen con el instalador de SnapCenter. Puede configurar SnapCenter para comprobar si hay actualizaciones disponibles.

El flujo de trabajo muestra las diferentes tareas necesarias para actualizar SnapCenter Server y los paquetes de plugins.




### Rutas de actualización admitidas

| Si se encuentra en la versión de SnapCenter Server… | Puede actualizar directamente el servidor de SnapCenter a… | Versiones de plugins compatibles |
|---|---|---|
| 4.2.x. | 4.3.x. | • 4.2.x.<br>• 4.3.x. |
| | 4.4.x. | • 4.4.x. |
| 4.3.x. | 4.4.x. | • 4.3.x.<br>• 4.4.x. |
| | 4.5.x. | • 4.5.x. |
| 4.4.x. | 4.5.x. | • 4.4.x.<br>• 4.5.x. |

Por ejemplo, si utiliza SnapCenter versión 4.2.x y desea actualizar a 4.5.x, primero debe actualizar a 4.4.x y, a continuación, realizar una actualización a 4.5.x.

Para obtener información sobre cómo actualizar el plugin de SnapCenter para VMware vSphere, consulte "Actualice el plugin de SnapCenter para VMware vSphere".

# Actualice el servidor SnapCenter

Puede utilizar el archivo ejecutable del instalador de SnapCenter Server para actualizar el servidor SnapCenter.

### Lo que necesitará

- El host del servidor de SnapCenter debe estar actualizado con las actualizaciones de Windows y no tener reinicios del sistema pendientes.
- Debe asegurarse de que no existan otras operaciones en ejecución antes de iniciar la operación de actualización.
- Debe realizar un backup de la base de datos del repositorio de SnapCenter (MySQL) después de asegurarse de que no exista ningún trabajo en ejecución.

  Para obtener más información, consulte "Realice un backup del repositorio de SnapCenter".

- Es necesario realizar un backup de todos los archivos de configuración de SnapCenter que se modificaron en el host SnapCenter Server o en el host del plugin.

  Ejemplos de archivos de configuración de SnapCenter: SnapDriveService.exe.config, SMCoreServiceHost.exe.config, etc.

### Acerca de esta tarea

- Durante la actualización, el host se pone automáticamente en modo de mantenimiento para evitar que el

host no ejecute ninguno de los trabajos programados. Después de la actualización, el host se extrae automáticamente del modo de mantenimiento.

- Antes de iniciar la operación de actualización, si ha colocado manualmente el host en modo de mantenimiento, después de la actualización debe desconectar manualmente el host del modo de mantenimiento haciendo clic en **hosts** > **Activar programa**.
- Pasos*

1. Descargue el paquete de instalación del servidor SnapCenter desde el sitio de soporte de NetApp.

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. Cree una copia del archivo web.config que se encuentra en C:\Program Files\NetApp\SnapCenter WebApp.
3. Exporte las programaciones de SnapCenter relacionadas con el host del plugin desde la programación de tareas de Windows para poder usarlo para restaurar las programaciones si no se realiza la actualización.

   ```
   md d:\\SCBackup``schtasks /query /xml /TN taskname >>
   "D:\SCBackup\taskname.xml"
   ```

4. Cree el volcado de la base de datos MySQL de SnapCenter si no está configurado el backup del repositorio.

   ```
   md d:\\SCBackup``mysqldump --all-databases --single-transaction --add-drop
   -database --triggers --routines --events -u root -p >
   D:\SCBackup\SCRepoBackup.dmp
   ```

   Cuando se le solicite, escriba la contraseña.

5. Inicie la actualización del servidor SnapCenter haciendo doble clic en el archivo .exe descargado.

   Después de iniciar la actualización, se realizan todas las comprobaciones previas y, si no se cumplen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes. Puede ignorar los mensajes de advertencia y continuar con la instalación. Sin embargo, se deben solucionar los errores.

   > SnapCenter seguirá utilizando la contraseña existente de la base de datos del repositorio de MySQL Server proporcionada durante la instalación de la versión anterior de SnapCenter Server.

6. Haga clic en **Actualizar**.

   En cualquier momento si hace clic en el botón **Cancelar**, el flujo de trabajo de actualización se cancelará. No se realizará la reversión del servidor SnapCenter al estado anterior.

**Mejor práctica:** debe cerrar sesión y luego iniciar sesión en SnapCenter, o cerrar y luego abrir un nuevo navegador para acceder a la GUI de SnapCenter.

### Después de terminar

- Si el plugin se instala mediante un usuario sudo, debe copiar las claves sha224 disponibles en *C:\ProgramData\NetApp\SnapCenter\Package Repository\oracle_checksum.txt* para actualizar el archivo

*/etc/sudoers*.

- Debe ejecutar una detección nueva de los recursos que hay en los hosts.

  Si el estado del host se muestra como detenido, puede esperar algún momento y realizar una detección nueva. También puede cambiar el valor del parámetro **HostRefreshInterval** (el valor predeterminado es 3600 segundos) a cualquier valor superior a 10 minutos.

- Si surge un error en la actualización, debe limpiar la instalación que ha fallado, reinstalar la versión anterior de SnapCenter y, a continuación, restaurar la base de datos NSM para restablecer su estado anterior.
- Después de actualizar el host del servidor de SnapCenter, también debe actualizar los plugins antes de añadir cualquier sistema de almacenamiento.

# Actualice los paquetes de plugins

Los paquetes de plugins se distribuyen como parte de la actualización de SnapCenter.

### Lo que necesitará

- Si es usted un usuario que no tiene categoría de usuario raíz pero sí tiene acceso a equipos Linux, debe actualizar el archivo */etc/sudoers* con los valores de la suma de verificación más recientes antes de ejecutar la operación de actualización.
- De forma predeterminada, SnapCenter detecta JAVA_HOME del entorno. Si desea utilizar UN JAVA_HOME fijo y si va a actualizar los plugins en un host Linux, debe añadir manualmente el parámetro SKIP_JAVAHOME_UPDATE en el archivo *spl.properties* ubicado en */var/opt/snapcenter/spl/etc/* y establecer el valor en TRUE.

  El valor de JAVA_HOME se actualiza cuando se actualiza el plugin o cuando se reinicia el servicio del cargador de plugins de SnapCenter (SPL). Antes de actualizar o reiniciar el SPL, si añade el parámetro SKIP_JAVAHOME_UPDATE y establece el valor en TRUE, el valor de JAVA_HOME no se actualiza.

- Es necesario tener un backup de todos los archivos de configuración de SnapCenter que se modificaron en el host de SnapCenter Server o en el host del plugin.

  Ejemplos de archivos de configuración de SnapCenter: SnapDriveService.exe.config, SMCoreServiceHost.exe.config, etc.

### Acerca de esta tarea

- El procedimiento de actualización sitúa su host Windows, Linux o AIX en modo «mantenimiento», lo que evita que el host ejecute cualquier trabajo programado.

  Para obtener información sobre cómo actualizar el plugin de SnapCenter para VMware vSphere, consulte "Actualice el plugin de SnapCenter para VMware vSphere".

- Pasos*

  1. En el panel de navegación izquierdo, haga clic en **hosts** > **Managed hosts**.
  2. Actualice los hosts realizando una de las siguientes tareas:
     - Si la columna Estado general muestra ""actualización disponible"" para uno de los hosts, haga clic en el nombre de host y realice lo siguiente:

i. Haga clic en **más opciones**.

ii. Seleccione **Skip prechecks** si no desea validar si el host cumple los requisitos para actualizar el plugin.

iii. Haga clic en **Actualizar**.

- Si desea actualizar varios hosts, seleccione todos los hosts, haga clic en Y, a continuación, haga clic en **Actualizar** > **Aceptar**.

> Todos los plugins del paquete se seleccionan, pero solo los que se habían instalado con la versión anterior de SnapCenter se actualizan. El resto de plugins no se instalarán. Debe utilizar la opción **Add plug-ins** para instalar cualquier complemento nuevo.

Si no ha seleccionado la casilla de comprobación **Skip prechecks, se analiza el host para verificar si cumple los requisitos para instalar el plugin. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes. Después de solucionar el problema, haga clic en *Actualizar**.

> Si el error está relacionado con el espacio en disco o RAM, puede actualizar el archivo web.config que está situado en C:\Program Files\NetApp\SnapCenter WebApp o los archivos de configuración de PowerShell que están situados en C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter\ para modificar los valores predeterminados. Si el error está relacionado con el resto de parámetros, debe solucionarlo y a continuación, validar de nuevo los requisitos.

# Desinstale SnapCenter Server y los plugins

## Desinstale los paquetes de plugins de SnapCenter

### Requisitos previos para quitar un host

Puede quitar hosts y desinstalar plugins individuales o paquetes de plugins por medio de la interfaz gráfica de usuario de SnapCenter. También puede desinstalar plugins individuales o paquetes de plugins de hosts remotos por medio de la interfaz de línea de comandos (CLI) en el host SnapCenter Server o usar la opción Windows **Desinstalar un programa** localmente en cualquier host.

Antes de quitar un host de servidor SnapCenter, debe completar los requisitos previos.

- Debe iniciar sesión como administrador.
- Si utiliza plugins de SnapCenter personalizados, debe eliminar todos los clones de SnapCenter que están asociados con el host.
- Debe asegurarse de que no existan trabajos de detección en ejecución en el host.
- Debe asignarse un rol con los permisos necesarios para eliminar todos los objetos asociados con el host. De lo contrario, la operación de eliminación fallará.
- Debe confirmar la huella digital si la clave SSH se modificó después de añadir el host a SnapCenter.
- También debe confirmar la huella digital si el host de SnapCenter se actualizó de una versión posterior de SnapCenter, pero el host del plugin sigue ejecutando una versión anterior del plugin.

#### Requisitos previos para quitar un host mediante el control de acceso basado en roles

- Debe haber iniciado sesión mediante un rol de RBAC que tenga permisos de lectura, eliminación de hosts, instalación, desinstalación de plugins y eliminación de objetos.

  Los objetos pueden ser de clonado, backup, grupos de recursos, sistema de almacenamiento, etc.

- Debe haber añadido el usuario de RBAC al rol de RBAC.
- Debe asignar el usuario de RBAC al host, plugin, credencial, grupos de recursos y sistema de almacenamiento (para clones) que desee eliminar.
- Debe haber iniciado sesión en SnapCenter como usuario de RBAC.

#### Requisitos previos para quitar un host con clones asociados de la operación de ciclo de vida de clones

- Debe haber creado trabajos de clonado mediante la gestión del ciclo de vida de clones para las bases de datos de SQL.
- Debe haber creado un rol de RBAC con los siguientes permisos: Lectura y eliminación de clones, lectura y eliminación de recursos, lectura y eliminación de grupos de recursos, lectura y eliminación de almacenamiento, lectura y eliminación de aprovisionamiento, montaje, desmontaje, instalación y desinstalación de plugins, y lectura y eliminación de hosts.
- Debe haber asignado el usuario de RBAC al rol de RBAC.
- Debe haber asignado el usuario de RBAC al host, plugin de SnapCenter para Microsoft SQL Server,

credencial, grupo de recursos de ciclo de vida de clones y sistema de almacenamiento.

- Debe haber iniciado sesión en SnapCenter como usuario de RBAC.

Para obtener más información sobre cómo desinstalar el plugin de SnapCenter para VMware vSphere, consulte "Quite el plugin de SnapCenter para VMware vSphere".

## Quitar un host

Cuando SnapCenter Server quita un host, primero elimina los backups, clones, trabajos de clonado, grupos de recursos y recursos que figuran para ese host en la página SnapCenter Resources. A continuación, desinstala los paquetes de plugins del host.

**Acerca de esta tarea**

- Si elimina un host, los backups, clones y grupos de recursos asociados con el host también se eliminan.
- Al quitar los grupos de recursos, se eliminan también todas las programaciones asociadas.
- Si se elimina un host que tiene un grupo de recursos compartido con otro host, también se elimina el grupo de recursos.
- Debe utilizar el cmdlet *Remove-SmHost* para quitar los hosts de plugin que se decomisionan o no se pueden acceder a ellos.

  La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software"

- El tiempo requerido para quitar un host depende de la cantidad de backups y de la configuración de retención. Esto es debido a que las copias de Snapshot se eliminan de cada una de las controladoras y se borran los metadatos.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione el host que desea eliminar y, a continuación, haga clic en **Quitar**.
  4. En el caso de clústeres RAC Oracle, para eliminar el software SnapCenter de todos los hosts del clúster, seleccione **incluir todos los hosts del cluster**.

     También puede quitar un nodo de un clúster y, de esa manera, quitar todos los nodos uno por uno.

  5. Haga clic en **Aceptar**.

Cuando desinstala y vuelve a instalar los plugins de host en un clúster, los recursos del clúster no se detectan de forma automática. Seleccione el nombre de host del clúster y, a continuación, haga clic en **Actualizar recursos** para detectar automáticamente los recursos del clúster.

## Desinstale plugins mediante la interfaz gráfica de usuario de SnapCenter

Cuando decide que ya no requiere un plugin individual o un paquete de plugins, puede desinstalarlo por medio de la interfaz de SnapCenter.

### Lo que necesitará

- Primero debe quitar los grupos de recursos correspondientes al paquete de plugins que vaya a desinstalar.
- Tiene que desconectar las políticas asociadas a los grupos de recursos correspondientes al paquete de plugins que vaya a desinstalar.

### Acerca de esta tarea

Puede desinstalar plugins individuales. Por ejemplo, quizás necesite desinstalar el plugin de SnapCenter para Microsoft SQL Server porque un host se está quedando sin recursos y quiere moverlo a un host más potente. También puede desinstalar paquetes de plugins enteros. Por ejemplo, quizás necesite desinstalar el paquete de plugins de SnapCenter para Linux, que incluye el plugin de SnapCenter para base de datos de Oracle y el plugin de SnapCenter para UNIX.

- La operación de quitar un host implica desinstalar todos los plugins.

  Cuando quita un host de SnapCenter, SnapCenter desinstalará todos los paquetes de plugins que haya en el host antes de quitar el host.

- La interfaz gráfica de usuario de SnapCenter quita los plugins de cada host uno por uno.

  Si utiliza la interfaz gráfica de usuario de SnapCenter, solamente puede desinstalar los plugins de un host cada vez. Sin embargo, puede tener varias operaciones de desinstalación que se ejecuten simultáneamente.

  También puede desinstalar un plugin de varios hosts mediante el cmdlet *Uninstall-SmHostPackage* y los parámetros requeridos. La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

> Desinstalar el paquete de plugins de SnapCenter para Windows de un host donde esté instalado el servidor SnapCenter dañará la instalación de SnapCenter Server. No desinstale el paquete de plugins de SnapCenter para Windows a menos que tenga la seguridad de que ya no requiere SnapCenter Server.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. En la página Managed hosts, seleccione el host desde el cual desea desinstalar el plugin o paquete de plugins.
  4. Junto al complemento que desea eliminar, haga clic en **Quitar** > **Enviar**.

### Después de terminar

Debe esperar 5 minutos antes de reinstalar el plugin en ese host. Este periodo es suficiente para que la interfaz gráfica de usuario de SnapCenter actualice el estado del host gestionado. Si procede a reinstalar de inmediato el plugin, la instalación no se desarrollará correctamente y provocará un error.

Si va a desinstalar el paquete de plugins de SnapCenter para Linux, los archivos de registro específicos de la desinstalación están disponibles en: */custom_location/snapcenter/log*.

## Desinstale los plugins de Windows mediante el cmdlet de PowerShell

Puede desinstalar plugins individuales o desinstalar paquetes de plugins enteros de uno o más hosts por medio del cmdlet *Uninstall-SmHostPackage* en la interfaz de línea de comandos del host de SnapCenter Server.

Es necesario que previamente haya iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host del que desee desinstalar los plugins.

- Pasos*
  1. Inicie PowerShell.
  2. En el host del servidor SnapCenter, introduzca el comando: *Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME* y, a continuación, introduzca sus credenciales.
  3. Desinstale los plugins de Windows mediante el cmdlet *Uninstall-SmHostPackage* y los parámetros necesarios.

     La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Como alternativa, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

## Desinstale los plugins localmente en un host

Puede desinstalar los plugins de SnapCenter localmente de un host si no puede acceder al host desde el servidor SnapCenter.

**Acerca de esta tarea**

La práctica recomendada para desinstalar plugins individuales o paquetes de plugins es utilizar la interfaz gráfica de usuario de SnapCenter o usar el cmdlet Uninstall-SmHostPackage en la interfaz de línea de comandos del host SnapCenter Server. Estos procedimientos ayudan al servidor SnapCenter a mantenerse actualizado con cualquier cambio.

Sin embargo, es posible que tenga una rara necesidad de desinstalar los plugins localmente. Por ejemplo, quizás haya ejecutado un trabajo de desinstalación desde SnapCenter Server, pero el trabajo generó un error, o tal vez desinstaló SnapCenter Server y los plugins huérfanos permanecen aún en el host.

Desinstalar un paquete de plugins localmente en un host no elimina los datos asociados con el host, como los trabajos programados y los metadatos de backups.

No trate de desinstalar el paquete de plugins de SnapCenter para Windows localmente desde Control Panel. Debe utilizar la interfaz gráfica de usuario de SnapCenter para asegurarse de que el plugin de SnapCenter para Microsoft Windows se desinstala correctamente.

- Pasos*
  1. En el sistema host, acceda al Panel de control y haga clic en **Desinstalar un programa**.
  2. En la lista de programas, seleccione el complemento SnapCenter o el paquete de plugins que desee desinstalar y haga clic en **Desinstalar**.

     Windows desinstalará todos los plugins incluidos en el paquete de plugins.

### Desinstale el paquete de plugins para Linux o AIX mediante la CLI

Puede desinstalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX mediante la interfaz de línea de comandos.

**Lo que necesitará**

- Asegúrese de eliminar los trabajos programados
- Asegúrese de que se han completado todos los trabajos en ejecución.

**Paso**

Ejecute */custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall* para desinstalar.

# Desinstale el servidor SnapCenter

Si ya no desea utilizar el servidor SnapCenter para administrar los trabajos de protección de datos, puede desinstalar el servidor SnapCenter mediante el Panel de control de programas y características del host del servidor SnapCenter. Al desinstalar el servidor SnapCenter se quitan todos sus componentes.

**Lo que necesitará**

- Asegúrese de tener al menos 2 GB de espacio libre en la unidad donde está instalado el servidor SnapCenter.
- Asegúrese de que no se quita el dominio en el que está instalado el servidor SnapCenter.

  Si quita el dominio donde se instaló el servidor SnapCenter y, a continuación, intenta desinstalar, la operación falla.

- Debe haber realizado un backup de la base de datos del repositorio porque se limpiará y desinstalará la base de datos del repositorio.
- Pasos*
  1. En el host del servidor SnapCenter, desplácese hasta el Panel de control.
  2. Asegúrese de estar en la vista **Categoría**.
  3. En programas, haga clic en **Desinstalar un programa**.

     Se abrirá la ventana programas y características.

  4. Seleccione NetApp SnapCenter Server y haga clic en **Uninstall**.

     Desde SnapCenter 4.2, al desinstalar SnapCenter Server, se desinstalan todos los componentes incluidos la base de datos de repositorio de MySQL Server.

     - Para quitar el nodo NLB de un clúster NLB, se requiere reiniciar el host de SnapCenter. Si no reinicia el host, puede producirse un fallo cuando intente reinstalar SnapCenter Server.
     - Debe desinstalar manualmente .NET Framework que no se quita durante la desinstalación.

# Automatización mediante API de REST

## Información general de las API de REST

Las API DE REST pueden utilizarse para realizar varias operaciones de gestión de SnapCenter. Las API DE REST se exponen a través de la página web de Swagger.

Es posible acceder a la página web de Swagger disponible en *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* para mostrar la documentación de API DE REST, y también para emitir manualmente una llamada API.

Los plugins compatibles con las API DE REST son:

- Plugin para Microsoft SQL Server
- Plugin para base de datos SAP HANA
- Plugins personalizados

## Cómo acceder a la API DE REST de SnapCenter de forma nativa

Puede acceder a la API DE REST de SnapCenter directamente desde cualquier lenguaje de programación que admita un cliente REST. Entre las opciones de idiomas populares se incluyen Python, PowerShell y Java.

## Base de servicios web DE REST

La transferencia de estado representacional (REST) es un estilo para crear aplicaciones web distribuidas. Cuando se aplica al diseño de una API de servicios web, establece un conjunto de tecnologías y prácticas recomendadas para exponer recursos basados en servidor y administrar sus estados. Utiliza estándares y protocolos más utilizados para proporcionar una base flexible para la gestión de SnapCenter.

### Recursos y representación estatal

Los recursos son los componentes básicos de un sistema basado en la Web. Al crear una aplicación DE SERVICIOS web DE REST, las tareas de diseño más tempranas incluyen:

#### Identificación de recursos basados en sistemas o servidores

Cada sistema utiliza y mantiene los recursos. Un recurso puede ser un archivo, una transacción comercial, un proceso o una entidad administrativa. Una de las primeras tareas en el diseño de una aplicación basada en servicios web DE REST es identificar los recursos.

#### Definición de estados de recursos y operaciones estatales asociadas

Los recursos siempre se encuentran en uno de un número limitado de estados. Los estados, así como las operaciones asociadas utilizadas para influir en los cambios de estado, deben definirse claramente.

### Extremos de URI

Todos los recursos REST deben definirse y ponerse a disposición mediante un esquema de direccionamiento bien definido. Los extremos en los que se encuentran e identifican los recursos utilizan un identificador uniforme de recursos (URI).

El URI proporciona un marco general para crear un nombre único para cada recurso de la red. El Localizador uniforme de recursos (URL) es un tipo de URI que se utiliza con los servicios web para identificar y acceder a los recursos. Los recursos normalmente se exponen en una estructura jerárquica similar a un directorio de archivos.

### Mensajes HTTP

El Protocolo de transferencia de hipertexto (HTTP) es el protocolo utilizado por el cliente y servidor de servicios web para intercambiar mensajes de solicitud y respuesta sobre los recursos.

Como parte del diseño de una aplicación de servicios web, los métodos HTTP se asignan a los recursos y a las correspondientes acciones de administración del estado. HTTP no tiene estado. Por lo tanto, para asociar un conjunto de solicitudes y respuestas relacionadas como parte de una transacción, se debe incluir información adicional en los encabezados HTTP transportados con los flujos de datos de solicitud y respuesta.

### Formato JSON

Aunque la información se puede estructurar y transferir entre un cliente de servicios web y un servidor de varias maneras, la opción más popular es la notación de objetos JavaScript (JSON).

JSON es un estándar del sector para representar estructuras de datos simples en texto sin formato y se utiliza para transferir información de estado que describe los recursos. La API REST de SnapCenter utiliza JSON para formatear los datos transportados en el cuerpo de cada solicitud y respuesta de HTTP.

# Variables de entrada que controlan una solicitud API

Puede controlar cómo se procesa una llamada API mediante parámetros y variables definidas en la solicitud HTTP.

### Métodos HTTP

En la siguiente tabla, se muestran los métodos HTTP compatibles con la API DE REST de SnapCenter.

No todos los métodos HTTP están disponibles en cada extremo DE REST.

| Método HTTP | Descripción |
|---|---|
| OBTENGA | Recupera propiedades de objeto en una instancia o colección de recursos. |
| PUBLICAR | Crea una nueva instancia de recurso basada en la entrada proporcionada. |
| ELIMINAR | Elimina una instancia de recurso existente. |
| PUESTO | Modifica una instancia de recurso existente. |

## Solicitar encabezados

Debe incluir varios encabezados en la solicitud HTTP.

### Tipo de contenido

Si el cuerpo de la solicitud incluye JSON, este encabezado debe establecerse en *Application/json*.

### Acepte

Este encabezado debe establecerse en *Application/json*.

### Autorización

La autenticación básica se debe establecer con el nombre de usuario y la contraseña codificados como una cadena base64.

## Solicitar el cuerpo

El contenido del cuerpo de la solicitud varía en función de la llamada específica. El cuerpo de la solicitud HTTP consta de uno de los siguientes elementos:

- Objeto JSON con variables de entrada
- Vacío

## Filtrando objetos

Al emitir una llamada API que utilice GET, puede limitar o filtrar los objetos devueltos en función de cualquier atributo. Por ejemplo, puede especificar un valor exacto para que coincida:

```
<field>=<query value>
```

Además de una coincidencia exacta, hay otros operadores disponibles para devolver un conjunto de objetos sobre un rango de valores. La API REST de SnapCenter es compatible con los operadores de filtrado que se muestran en la tabla siguiente.

| Operador | Descripción |
|---|---|
| = | Igual a. |
| < | Menor que |
| > | Mayor que |
| ⇐ | Menor o igual que |
| >= | Mayor o igual que |
| ACTUALIZAR | O. |
| ! | No es igual a. |
| * | Comodín codicioso |

También puede devolver una colección de objetos basándose en si se establece o no un campo específico utilizando la palabra clave **null** o su negación **!null** como parte de la consulta.

Los campos que no están configurados generalmente se excluyen de consultas coincidentes.

## Solicitando campos de objeto específicos

De forma predeterminada, al emitir una llamada API mediante GET, sólo se devuelven los atributos que identifican de forma exclusiva el objeto o los objetos. Este conjunto mínimo de campos actúa como clave para cada objeto y varía según el tipo de objeto. Puede seleccionar propiedades de objeto adicionales mediante la `fields` parámetro de consulta de las siguientes formas:

#### Campos comunes o estándar

Especifique **Fields=*** para recuperar los campos de objeto más utilizados. Estos campos normalmente se mantienen en la memoria del servidor local o requieren poco procesamiento para acceder. Estas son las mismas propiedades que se devuelven para un objeto después de utilizar GET con una clave de ruta de URL (UUID).

#### Todos los campos

Especifique **Fields=**** para recuperar todos los campos de objeto, incluidos los que requieren procesamiento de servidor adicional para tener acceso.

#### Selección de campo personalizado

Utilice **Fields=<field_name>** para especificar el campo exacto que desea. Al solicitar varios campos, los valores deben separarse con comas sin espacios.

Como práctica recomendada, siempre debe identificar los campos específicos que desea. Sólo debe recuperar el conjunto de campos comunes o todos los campos cuando sea necesario. NetApp determina qué campos se clasifican como comunes y se devuelven con *fields=** en función del análisis de rendimiento interno. La clasificación de un campo puede cambiar en versiones futuras.

## Ordenar objetos del conjunto de resultados

Los registros de una colección de recursos se devuelven en el orden predeterminado definido por el objeto. Puede cambiar el pedido mediante `order_by` consulte el parámetro con el nombre del campo y la dirección de ordenación de la siguiente manera:

```
order_by=<field name> asc|desc
```

Por ejemplo, puede ordenar el campo de tipo en orden descendente seguido de id en orden ascendente:

```
order_by=type desc, id asc
```

- Si especifica un campo de ordenación pero no proporciona una dirección, los valores se ordenan en orden ascendente.
- Cuando se incluyan varios parámetros, los campos deben separarse con una coma.

## Paginación al recuperar objetos de una colección

Al emitir una llamada API mediante GET para acceder a una colección de objetos del mismo tipo, SnapCenter intenta devolver tantos objetos como sea posible basándose en dos restricciones. Puede controlar cada una

de estas restricciones utilizando parámetros de consulta adicionales en la solicitud. La primera restricción alcanzada para una solicitud GET específica termina la solicitud y, por lo tanto, limita el número de registros devueltos.

Si una solicitud finaliza antes de iterar todos los objetos, la respuesta contiene el vínculo necesario para recuperar el siguiente lote de registros.

#### Limitar el número de objetos

De forma predeterminada, SnapCenter devuelve un máximo de 10,000 objetos para UNA solicitud GET. Puede cambiar este límite utilizando el parámetro de consulta *max_Records* . Por ejemplo:

```
max_records=20
```

El número de objetos realmente devueltos puede ser menor que el máximo en efecto, basándose en la restricción de tiempo relacionada, así como en el número total de objetos del sistema.

#### Limitar el tiempo utilizado para recuperar los objetos

De forma predeterminada, SnapCenter devuelve tantos objetos como sea posible dentro del tiempo permitido para LA solicitud GET. El tiempo de espera predeterminado es 15 segundos. Puede cambiar este límite utilizando el parámetro de consulta *return_TIMEOUT*. Por ejemplo:

```
return_timeout=5
```

El número de objetos realmente devueltos puede ser menor que el máximo en efecto, basándose en la restricción relacionada en el número de objetos así como en el número total de objetos del sistema.

#### Reducción del conjunto de resultados

Si es necesario, puede combinar estos dos parámetros con parámetros de consulta adicionales para restringir el conjunto de resultados. Por ejemplo, el siguiente devuelve hasta 10 eventos de EMS generados después de la hora especificada:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Puede emitir varias solicitudes para desplazarse por los objetos. Cada llamada API posterior debe utilizar un nuevo valor de tiempo basado en el último evento del último conjunto de resultados.

## Propiedades de tamaño

Los valores de entrada utilizados con algunas llamadas API, así como ciertos parámetros de consulta son numéricos. En lugar de proporcionar un entero en bytes, puede usar de manera opcional un sufijo como se muestra en la siguiente tabla.

| Sufijo | Descripción |
|---|---|
| KB | Kilobytes de KB (1024 bytes) o kibibytes |
| MB | MB megabytes (KB x 1024 bytes) o mebibytes |
| GB | GB Gigabytes (MB x 1024 bytes) o gibibytes |
| TB | TB terabytes (GB x 1024 byes) o tebibytes |

| Sufijo | Descripción |
| --- | --- |
| PB | Petabytes de PB (TB x 1024 byes) o gibibytes |

# Interpretación de una respuesta API

Cada solicitud de API genera una respuesta al cliente. Debe examinar la respuesta para determinar si ha tenido éxito y recuperar datos adicionales según sea necesario.

## Código de estado HTTP

A continuación se describen los códigos de estado HTTP utilizados por la API DE REST de SnapCenter.

| Codificación | Descripción |
| --- | --- |
| 200 | OK indica éxito para las llamadas que no crean un nuevo objeto. |
| 201 | Se ha creado correctamente un objeto. El encabezado de ubicación de la respuesta incluye el identificador único del objeto. |
| 202 | Aceptado se ha iniciado Un trabajo en segundo plano para realizar la solicitud, pero aún no se ha completado. |
| 400 | Solicitud incorrecta la entrada de la solicitud no se reconoce o no es apropiada. |
| 401 | Se ha producido un error en la autenticación de usuario no autorizada. |
| 403 | El acceso prohibido se rechaza debido a un error de autorización (RBAC). |
| 404 | No se encuentra el recurso al que se hace referencia en la solicitud no existe. |
| 405 | Método no permitido el método HTTP en la solicitud no es compatible con el recurso. |
| 409 | Conflicto error al intentar crear un objeto porque primero se debe crear otro objeto o ya existe el objeto solicitado. |
| 500 | Error interno se ha producido un error interno general en el servidor. |

## Encabezados de respuesta

Se incluyen varios encabezados en la respuesta HTTP generada por SnapCenter.

### Ubicación

Cuando se crea un objeto, el encabezado de ubicación incluye la dirección URL completa del nuevo objeto, incluido el identificador único asignado al objeto.

### Tipo de contenido

Esto será normalmente `application/json`.

## Cuerpo de respuesta

El contenido del cuerpo de respuesta que resulta de una solicitud API varía en función del objeto, el tipo de procesamiento y el éxito o el fallo de la solicitud. La respuesta siempre se representa en JSON.

### Un solo objeto

Un solo objeto se puede devolver con un conjunto de campos basados en la solicitud. Por ejemplo, se puede usar GET para recuperar las propiedades seleccionadas de un clúster mediante el identificador único.

### Varios objetos

Se pueden devolver varios objetos de una colección de recursos. En todos los casos, existe un formato coherente utilizado, con `num_records` indica el número de registros y registros que contienen una matriz de las instancias de objeto. Por ejemplo, puede recuperar los nodos definidos en un clúster específico.

### Objeto de trabajo

Si una llamada API se procesa de forma asíncrona, se devuelve un objeto Job que ancla la tarea en segundo plano. Por ejemplo, la solicitud DE REVISIÓN utilizada para actualizar la configuración del clúster se procesa de forma asíncrona y devuelve un objeto Job.

### Objeto de error

Si se produce un error, siempre se devuelve un objeto error. Por ejemplo, recibirá un error al intentar cambiar un campo no definido para un clúster.

### Vacío

En ciertos casos, no se devuelven datos y el cuerpo de respuesta incluye un objeto JSON vacío.

## Errores

Si se produce un error, se devuelve un objeto de error en el cuerpo de respuesta.

### Formato

Un objeto de error tiene el siguiente formato:

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

Puede utilizar el valor del código para determinar el tipo o la categoría de error general y el mensaje para determinar el error específico. Si está disponible, el campo de destino incluye la entrada de usuario específica

asociada al error.

**códigos de error comunes**

Los códigos de error comunes se describen en la siguiente tabla. Las llamadas API específicas pueden incluir códigos de error adicionales.

| Codificación | Descripción |
|---|---|
| 409 | Ya existe un objeto con el mismo identificador. |
| 400 | El valor de un campo no es válido o falta, o se ha proporcionado un campo adicional. |
| 400 | La operación no es compatible. |
| 405 | No se puede encontrar un objeto con el identificador especificado. |
| 403 | Se deniega el permiso para realizar la solicitud. |
| 409 | El recurso está en uso. |

# API de REST compatibles

Los recursos disponibles a través de la API DE REST de SnapCenter están organizados en categorías, como se muestra en la página de documentación de API SnapCenter. A continuación se presenta una breve descripción de cada uno de los recursos con las rutas de recursos base, junto con otras consideraciones de uso adicionales si procede.

## Autor

Puede utilizar esta llamada API para iniciar sesión en el servidor SnapCenter. Esta API devuelve un token de autorización de usuario que se utiliza para autenticar solicitudes posteriores.

## Dominios

Puede usar estas llamadas API para realizar lo siguiente:

- recupere todos los dominios
- recuperar detalles de un dominio específico
- registre o cancele el registro de un dominio
- modificar un dominio

## Trabajos

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar todos los trabajos
- recuperar el estado de un trabajo
- cancelar o detener un trabajo

## Configuración

Puede usar estas llamadas API para realizar lo siguiente:

- registre, vea, modifique o quite una credencial
- configurar los ajustes de notificación

## Hosts

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar los detalles del host
- recupere el plugin instalado y sus detalles de recursos
- añada, quite o modifique un host de plugin
- instale o actualice los plugins

## Recursos

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar recursos
- crear, modificar o quitar recursos
- proteger un recurso
- realice un backup, restaure o clone un recurso

## Completos

Puede usar estas llamadas API para realizar lo siguiente:

- recupere los detalles de la copia de seguridad
- cambiar el nombre o eliminar backups

## Clones

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar detalles de clones
- eliminar clones

## Clanesplit

Puede usar estas llamadas API para realizar lo siguiente:

- recupere el estado de una operación de división de clones
- inicie o detenga una operación de división de clones

## Grupos de recursos

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar los detalles de un grupo de recursos
- crear, modificar o eliminar un grupo de recursos
- realice un backup de un grupo de recursos

## Normativas

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar los detalles de la política
- crear, modificar o eliminar políticas

## Reducida

Puede usar estas llamadas API para realizar lo siguiente:

- recupere los detalles de almacenamiento
- crear, modificar o eliminar un almacenamiento
- detectar recursos en un almacenamiento de
- cree o elimine un recurso compartido en el almacenamiento

## Share

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar los detalles de un recurso compartido
- cree o elimine un recurso compartido en el almacenamiento

## Complementos

Estas llamadas API se pueden usar para recuperar todos los plugins de un host y realizar diferentes operaciones.

## Leídos

Puede usar estas llamadas API para realizar lo siguiente:

- generar informes de backup, restauración, clonado y plugin
- agregar, ejecutar, eliminar o modificar programaciones

## Alertas

Puede usar estas llamadas API para realizar lo siguiente:

- recupere todas las alertas
- eliminar alertas

### RBAC

Puede usar estas llamadas API para realizar lo siguiente:

- recuperar detalles de usuarios, grupos y roles
- añadir usuarios
- crear, modificar o eliminar roles
- asignar o anular la asignación de roles y grupos

### Configuración

Puede usar estas llamadas API para realizar lo siguiente:

- ver los ajustes de configuración
- modifique las opciones de configuración

### CertificadosConfiguración

Puede usar estas llamadas API para realizar lo siguiente:

- vea el estado del certificado
- modifique la configuración del certificado

### Repositorio

Puede usar estas llamadas API para realizar lo siguiente:

- Realice un backup y restaure el repositorio de NSM
- Proteja y desproteja el repositorio NSM
- conmutación al respaldo
- Vuelva a generar el repositorio NSM

# Cómo acceder a las API de REST a través de la página web de API de Swagger

Las API DE REST se exponen a través de la página web de Swagger. Es posible acceder a la página web de Swagger para mostrar las API DE REST de SnapCenter Server, y también para emitir manualmente una llamada API. Es posible usar la API DE REST para ayudar a gestionar SnapCenter Server o para realizar operaciones de protección de datos.

Debe conocer la dirección IP o el nombre de dominio de gestión de la instancia de SnapCenter Server donde desea ejecutar las API de REST.

No se necesitan permisos especiales para ejecutar el cliente API de REST. Cualquier usuario puede acceder a la página web de Swagger. Los permisos respectivos en los objetos a los que se accede a través de la API DE REST se basan en el usuario que genera el token para iniciar sesión en la API DE REST.

- Pasos*

1. Desde un explorador, introduzca la URL para acceder a la página web de Swagger con el formato *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/*.

   Asegúrese de que la dirección URL de la API DE REST no tenga los caracteres siguientes: +, ., % y &.

2. En el campo **Explore** de Swagger, si la documentación de API de Swagger no se muestra automáticamente, escriba: *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/SnapCenter.yaml*
3. Haga clic en **explorar**.

   Se muestra una lista de los tipos de recursos o categorías de la API.

4. Haga clic en un tipo de recurso de la API para mostrar las API en ese tipo de recurso.

Si se produce un comportamiento inesperado al ejecutar las API DE REST de SnapCenter, puede usar los archivos de registro para identificar la causa del problema y resolverlo. Puede descargar los archivos de registro desde la interfaz de usuario de SnapCenter haciendo clic en **Monitor** > **Logs** > **Download**.

# Comience con la API DE REST

Es posible comenzar a usar rápidamente la API de REST de SnapCenter. El acceso a la API ofrece una cierta perspectiva antes de comenzar a utilizarla con los procesos de flujos de trabajo más complejos en una configuración en directo.

## Hola Mundo

Puede ejecutar un comando simple en su sistema para comenzar a utilizar la API DE REST de SnapCenter y confirmar su disponibilidad.

### Lo que necesitará

- Asegúrese de que la utilidad Curl está disponible en el sistema.
- La dirección IP o el nombre de host del servidor SnapCenter
- Nombre de usuario y contraseña para una cuenta con autoridad para acceder a la API DE REST de SnapCenter.

Si sus credenciales incluyen caracteres especiales, debe formatearlos de una forma que sea aceptable para Curl en función del shell que esté utilizando. Por ejemplo, puede insertar una barra diagonal inversa antes de cada carácter especial o envolver la totalidad `username:password` cadena entre comillas simples.

### Paso

En la interfaz de línea de comandos de, ejecute lo siguiente para recuperar la información del plugin:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Ejemplo:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

# Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

## Derechos de autor

"http://www.netapp.com/us/legal/copyright.aspx"

## 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.

"http://www.netapp.com/us/legal/netapptmlist.aspx"

## Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

"https://www.netapp.com/us/media/patents-page.pdf"

## Política de privacidad

"https://www.netapp.com/us/legal/privacypolicy/index.aspx"

## Traducción automática

Información importante sobre contenido localizado.

"https://www.netapp.com/company/legal/machine-translation/"

## Código abierto

Proporciona información acerca de los derechos de autor y las licencias de terceros utilizados en este producto. Su producto no utiliza necesariamente todos los componentes de software a los que se hace referencia a continuación.

"Aviso para SnapCenter 4.5"

**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.