Documentación de software SnapCenter

SnapCenter software

NetApp
February 20, 2026

This PDF was generated from https://docs.netapp.com/es-es/snapcenter/index.html on February 20, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de software SnapCenter . . . 1
Notas de la versión . . . 2
Notas de la versión . . . 2
Rutas de actualización admitidas para SnapCenter . . . 2
Manos a la obra . . . 3
Obtenga más información sobre el software SnapCenter . . . 3
Información general de SnapCenter . . . 3
Funciones de seguridad de SnapCenter . . . 7
Control de acceso basado en roles en SnapCenter . . . 9
Recuperación ante desastres en SnapCenter . . . 14
Licencias requeridas por SnapCenter . . . 15
SnapMirror sincronización activa en SnapCenter . . . 18
Conceptos clave de la protección de datos . . . 18
Aplicaciones y sistemas de almacenamiento compatibles con SnapCenter . . . 21
Métodos de autenticación para las credenciales de SnapCenter . . . 21
Operaciones de SnapCenter compatibles con sistemas ASA r2 . . . 23
Inicio rápido para software SnapCenter . . . 24
Instalar y configurar SnapCenter Server . . . 26
Prepare la instalación del servidor SnapCenter . . . 26
Requisitos para instalar el servidor SnapCenter . . . 26
Regístrese para acceder al software de SnapCenter . . . 33
Autenticación multifactor (MFA) . . . 34
Instale el servidor SnapCenter . . . 44
Instale el servidor de SnapCenter en el host de Windows . . . 44
Instale el servidor SnapCenter en el host Linux . . . 49
Registre SnapCenter . . . 53
Inicie sesión en SnapCenter mediante la autorización de RBAC . . . 53
Configurar el servidor SnapCenter . . . 57
Agregar y aprovisionar el sistema de almacenamiento . . . 57
Añada licencias estándar basadas en controladora de SnapCenter . . . 78
Configuración de la alta disponibilidad . . . 83
Configurar el control de acceso basado en roles (RBAC) . . . 87
Configure los ajustes del registro de auditoría . . . 116
Configure las conexiones MySQL protegidas con SnapCenter Server . . . 117
Configure la autenticación basada en certificados . . . 124
Habilite la autenticación basada en certificados . . . 124
Exporte certificados de entidad de certificación (CA) del servidor SnapCenter . . . 124
Importe el certificado de CA a los hosts del plugin de Windows . . . 125
Importe el certificado de CA en los hosts del plugin UNIX . . . 126
Exportar certificados SnapCenter . . . 127
Configurar certificado de CA para el host de Windows . . . 128
Genere un archivo CSR de certificado de CA . . . 128
Importar certificados de CA . . . 128

Obtenga la huella digital del certificado de CA . . . 129
Configure el certificado de CA con servicios de plugins de host de Windows . . . 130
Configurar el certificado de CA con el sitio SnapCenter . . . 131
Habilite los certificados de CA para SnapCenter . . . 131
Configurar certificado de CA para el host Linux . . . 132
Configure el certificado nginx . . . 132
Configure el certificado de registro de auditoría . . . 132
Configurar el certificado de SnapCenter . . . 133
Configure y habilite la comunicación SSL bidireccional en el host Windows . . . 133
Configure la comunicación SSL bidireccional en el host de Windows . . . 133
Habilite la comunicación SSL bidireccional en el host Windows . . . 136
Configure y habilite la comunicación SSL bidireccional en el host Linux . . . 137
Configure la comunicación SSL bidireccional en el host Linux . . . 137
Active la comunicación SSL en el host Linux . . . 139
Configure Active Directory, LDAP y LDAPS . . . 139
Registrar dominios de Active Directory que no son de confianza . . . 139
Configure los grupos de aplicaciones de IIS para habilitar los permisos de lectura de Active Directory . . . 141
Configure el certificado de cliente de CA para LDAPS . . . 141
Proteger bases de datos de Microsoft SQL Server . . . 143
Plugin de SnapCenter para Microsoft SQL Server . . . 143
Información general sobre el plugin de SnapCenter para Microsoft SQL Server . . . 143
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft SQL Server . . . 143
Funciones del plugin de SnapCenter para Microsoft SQL Server . . . 144
Compatibilidad con asignación de LUN asimétrica en clústeres de Windows . . . 145
Tipos de almacenamiento compatibles con el plugin de SnapCenter para Microsoft SQL Server . . . 146
Recomendaciones sobre distribución de almacenamiento para el plugin de SnapCenter para Microsoft SQL Server . . . 149
Privilegios mínimos de ONTAP requeridos para el plugin de SQL . . . 151
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para SQL Server . . . 153
Estrategia de backup para recursos de SQL Server . . . 154
Estrategia de restauración para SQL Server . . . 159
Defina una estrategia de clonación para SQL Server . . . 162
Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server . . . 163
Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft SQL Server . . . 163
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft SQL Server . . . 163
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 164
Configure credenciales para el paquete de plugins de SnapCenter para Windows . . . 165
Configure las credenciales para un recurso individual de SQL Server . . . 166
Configurar GMSA en Windows Server 2016 o posterior . . . 168
Instale el plugin de SnapCenter para Microsoft SQL Server . . . 170
Configurar certificado de CA . . . 176
Configure la recuperación ante desastres . . . 179
Instale el plugin de SnapCenter para VMware vSphere . . . 181
Implemente el certificado de CA . . . 181

Configure el archivo CRL . . . 181
Prepárese para la protección de datos . . . 182
Requisitos previos para utilizar el plugin de SnapCenter para Microsoft SQL Server . . . 182
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger SQL Server . . . 183
Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad . . . 183
Flujo de trabajo de backup . . . 184
Determine si hay recursos disponibles para backup . . . 185
Migrar recursos al sistema de almacenamiento de NetApp . . . 187
Crear políticas de backup para bases de datos de SQL Server . . . 189
Crear grupos de recursos y asociar políticas para SQL Server . . . 195
Cree grupos de recursos y habilite la protección secundaria para recursos de Microsoft SQL Server en sistemas ASA R2 . . . 198
Requisitos para realizar backups de recursos de SQL . . . 201
Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell . . . 201
Realice backups de recursos de SQL . . . 202
Realizar un backup de grupos de recursos de SQL Server . . . 208
Supervise las operaciones de backup de los recursos de SQL en la página SnapCenter Jobs . . . 209
Cancelar las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server . . . 210
Consulte los backups y los clones de SQL Server en la página Topology . . . 211
Borre el número de backup secundario con cmdlets de PowerShell . . . 213
Restaure recursos de SQL Server . . . 214
Restaure el flujo de trabajo . . . 214
Requisitos para restaurar una base de datos . . . 214
Restaurar backups de base de datos de SQL Server . . . 215
Restaurar una base de datos de SQL Server a partir de almacenamiento secundario . . . 222
Restaurar recursos mediante los cmdlets de PowerShell . . . 223
Propagación de bases de datos de grupos de disponibilidad . . . 225
Supervisar operaciones de restauración de recursos de SQL . . . 226
Cancelar las operaciones de restauración de recursos de SQL . . . 227
Clone recursos de bases de datos de SQL Server . . . 227
Flujo de trabajo de clonado . . . 228
Clonar a partir de un backup de base de datos de SQL Server . . . 228
Ejecute el ciclo de vida del clon . . . 236
Supervisar operaciones de clonado de bases de datos de SQL . . . 239
Cancelar las operaciones de clonado de recursos SQL . . . 240
Divida un clon . . . 240
Proteger las bases de datos SAP HANA . . . 242
Plugin de SnapCenter para base de datos SAP HANA . . . 242
Información general sobre el plugin de SnapCenter para bases de datos de SAP HANA . . . 242
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para base de datos SAP HANA . . . 242
Funciones del plugin de SnapCenter para base de datos SAP HANA . . . 243
Tipos de almacenamiento compatibles con el plugin de SnapCenter para base de datos SAP HANA . . . 243
Privilegios mínimos ONTAP requeridos para el plugin de SAP HANA . . . 244
Preparar los sistemas de almacenamiento para la replicación SnapMirror y SnapVault para las bases

de datos SAP HANA . . . 247
Estrategia de backup para las bases de datos SAP HANA . . . 247
Estrategia de restauración y recuperación para bases de datos SAP HANA . . . 251
Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA . . . 253
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA . . . 253
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA . . . 254
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 257
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 258
Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA . . . 259
Configurar GMSA en Windows Server 2016 o posterior . . . 262
Instale el plugin de SnapCenter para base de datos SAP HANA . . . 263
Configurar certificado de CA . . . 269
Instale el plugin de SnapCenter para VMware vSphere . . . 277
Implemente el certificado de CA . . . 277
Configure el archivo CRL . . . 277
Prepárese para la protección de datos . . . 277
Requisitos previos para usar el plugin de SnapCenter para base de datos SAP HANA . . . 277
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger bases de datos SAP HANA . . . 278
Realice un backup de los recursos de SAP HANA . . . 279
Realice un backup de los recursos de SAP HANA . . . 279
Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA . . . 280
Descubra recursos y prepare contenedores de bases de datos multitenant para la protección de datos . . . 280
Añada recursos manualmente al host del plugin . . . 283
Crear políticas de backup para bases de datos SAP HANA . . . 285
Crear grupos de recursos y añadir políticas . . . 291
Cree grupos de recursos y habilite la protección secundaria para recursos SAP HANA en sistemas ASA R2 . . . 295
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos SAP HANA . . . 298
Realice un backup de las bases de datos SAP HANA . . . 299
Realice un backup de los grupos de recursos . . . 307
Supervisar las operaciones de backup de las bases de datos SAP HANA . . . 307
Cancele las operaciones de backup para SAP HANA . . . 308
Consulte los backups y los clones de la base de datos SAP HANA en la página Topology . . . 309
Restaure bases de datos de SAP HANA . . . 311
Restaure el flujo de trabajo . . . 311
Restaurar y recuperar un backup de recurso añadido manualmente . . . 312
Restaurar y recuperar un backup de base de datos detectado automáticamente . . . 316
Restaurar recursos mediante los cmdlets de PowerShell . . . 320
Supervisar las operaciones de restauración de bases de datos SAP HANA . . . 322
Clonar backups de recursos SAP HANA . . . 323

Flujo de trabajo de clonado . . . 323
Clonar un backup de base de datos SAP HANA . . . 324
Supervise las operaciones de clonado de base de datos SAP HANA . . . 328
Divida un clon . . . 328
Elimine o divida los clones de las bases de datos SAP HANA después de actualizar SnapCenter . . . 330
Proteger bases de datos de Oracle . . . 331
Información general del plugin de SnapCenter para base de datos de Oracle . . . 331
Qué puede hacer con el plugin para base de datos de Oracle . . . 331
Funciones del plugin para base de datos de Oracle . . . 331
Tipos de almacenamiento compatibles con el plugin para bases de datos de Oracle . . . 333
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para Oracle . . . 335
Privilegios mínimos requeridos de ONTAP para el plugin para Oracle . . . 335
Instale el plugin de SnapCenter para base de datos de Oracle . . . 337
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos de Oracle . . . 338
Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux o AIX . . . 338
Añada hosts e instale el paquete de plugins para Linux o AIX mediante la interfaz gráfica de usuario . . . 348
Formas alternativas de instalar el paquete de plugins para Linux o AIX . . . 352
Configure el servicio de cargador de plugins de SnapCenter . . . 355
Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux . . . 358
Habilite certificados de CA para plugins . . . 361
Importe datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter . . . 361
Instale el plugin de SnapCenter para VMware vSphere . . . 367
Implemente el certificado de CA . . . 368
Configure el archivo CRL . . . 368
Preparar la protección de bases de datos de Oracle . . . 368
Realice backups de bases de datos de Oracle . . . 369
Descripción general del procedimiento de copia de seguridad . . . 369
Información de configuración de backup . . . 370
Requisitos para realizar backups de una base de datos de Oracle . . . 383
Detectar las bases de datos de Oracle disponibles para backup . . . 383
Crear políticas de backup para bases de datos de Oracle . . . 385
Crear grupos de recursos y vincular políticas para bases de datos de Oracle . . . 392
Crear grupos de recursos y habilitar la protección secundaria para recursos de Oracle en sistemas ASA R2 . . . 395
Realice backup de recursos de Oracle . . . 397
Realice backups de grupos de recursos de bases de datos de Oracle . . . 400
Supervisar la copia de seguridad de Oracle Database . . . 401
Otras operaciones de backup . . . 402
Montar y desmontar backups de bases de datos . . . 406
Montar un backup de base de datos . . . 407
Desmontar un backup de base de datos . . . 408
Restaurar y recuperar bases de datos de Oracle . . . 409
Restaure el flujo de trabajo . . . 409

Definir una estrategia de restauración y recuperación para bases de datos de Oracle . . . 409
Variables de entorno predefinidas para restaurar scripts previos y posteriores específicos . . . 414
Requisitos para restaurar una base de datos de Oracle . . . 415
Restaurar y recuperar bases de datos de Oracle . . . 416
Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico . . . 422
Restaure y recupere una base de datos conectable mediante la recuperación de un momento específico . . . 423
Restaure y recupere bases de datos de Oracle con comandos de UNIX . . . 426
Supervisar las operaciones de restauración de bases de datos de Oracle . . . 426
Cancelar operaciones de restauración de bases de datos de Oracle . . . 427
Clone la base de datos de Oracle . . . 428
Flujo de trabajo de clonado . . . 428
Defina una estrategia de clonado para bases de datos de Oracle . . . 429
Variables de entorno predefinidas para el script previo y script posterior específicos de clon . . . 430
Requisitos para clonar una base de datos de Oracle . . . 432
Clonar el backup de una base de datos de Oracle . . . 434
Clonar una base de datos conectable . . . 443
Clonar backups de bases de datos de Oracle con comandos UNIX . . . 448
Divida el clon de una base de datos de Oracle . . . 449
Clon dividido de una base de datos conectable . . . 450
Supervise las operaciones de clonado de las bases de datos de Oracle . . . 450
Actualizar un clon . . . 451
Eliminar el clon de una base de datos conectables . . . 452
Gestione los volúmenes de aplicaciones . . . 453
¿Qué son volúmenes de aplicación . . . 453
Añada volúmenes de la aplicación . . . 453
Aplicación de backup para volúmenes . . . 454
Clone el backup de volumen de la aplicación . . . 457
Protección de sistemas de archivos Windows . . . 459
Conceptos del plugin de SnapCenter para Microsoft Windows . . . 459
Información general sobre el plugin de SnapCenter para Microsoft Windows . . . 459
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft Windows . . . 459
Funciones del plugin de SnapCenter para Windows . . . 460
Cómo hace SnapCenter para realizar backup de sistemas de archivos Windows . . . 461
Tipos de almacenamiento compatibles con el plugin de SnapCenter para Microsoft Windows . . . 461
Privilegios mínimos de ONTAP requeridos para el plugin de Windows . . . 464
Preparar los sistemas de almacenamiento para la replicación con SnapMirror y SnapVault . . . 466
Defina una estrategia de backup para sistemas de archivos de Windows . . . 467
Orígenes y destinos de clones para sistemas de archivos Windows . . . 469
Instale el plugin de SnapCenter para Microsoft Windows . . . 469
Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Windows . . . 469
Requisitos de instalación del plugin de SnapCenter para Microsoft Windows . . . 469
Añada hosts e instale el plugin de SnapCenter para Microsoft Windows . . . 474
Instale el plugin de SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets

de PowerShell . . . 478
Instale el plugin de SnapCenter para Microsoft Windows silenciosamente desde la línea de comandos 478
Supervise el estado de instalación del paquete de plugins de SnapCenter . . . 480
Configure el certificado de CA . . . 481
Instale el plugin de SnapCenter para VMware vSphere . . . 484
Implemente el certificado de CA . . . 484
Configure el archivo CRL . . . 484
Realizar backup de sistemas de archivos Windows . . . 484
Realizar backup de sistemas de archivos Windows . . . 485
Determinar la disponibilidad de recursos para los sistemas de archivos Windows . . . 486
Crear políticas de backup para sistemas de archivos Windows . . . 487
Crear grupos de recursos para sistemas de archivos Windows . . . 490
Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Windows en sistemas ASA R2 . . . 493
Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell . . . 495
Realice el backup de un solo recurso bajo demanda para sistemas de archivos Windows . . . 496
Realizar un backup de grupos de recursos para sistemas de archivos Windows . . . 501
Supervisar las operaciones de backup . . . 502
Cancele las operaciones de backup . . . 503
Consulte los backups y los clones relacionados en la página Topology . . . 504
Borre el número de backup secundario con cmdlets de PowerShell . . . 506
Restaurar sistemas de archivos Windows . . . 507
Restaurar backups de sistemas de archivos Windows . . . 507
Restaurar recursos mediante los cmdlets de PowerShell . . . 512
Supervisar operaciones de restauración . . . 515
Cancele las operaciones de restauración . . . 516
Clonar sistemas de archivos Windows . . . 517
Clonar desde un backup de sistema de archivos Windows . . . 517
Supervise las operaciones de clonación . . . 523
Cancele las operaciones de clonado . . . 524
Divida un clon . . . 525
Proteger las bases de datos de Microsoft Exchange Server . . . 527
Conceptos del plugin de SnapCenter para Microsoft Exchange Server . . . 527
Información general sobre el plugin de SnapCenter para Microsoft Exchange Server . . . 527
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft Exchange Server . . . 528
Tipos de almacenamiento compatibles con el complemento SnapCenter para Microsoft Exchange Server . . . 528
Privilegios mínimos de ONTAP requeridos para el plugin de Exchange . . . 529
Preparar los sistemas de almacenamiento para la replicación con SnapMirror y SnapVault . . . 532
Defina una estrategia de backup para recursos de servidor de Exchange . . . 532
Definir una estrategia de restauración para bases de datos de Exchange . . . 535
Instale el plugin de SnapCenter para Microsoft Exchange Server . . . 536
Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Exchange Server . . . 536
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft Exchange

Server . . . 537
Configure credenciales para el plugin de SnapCenter para Windows . . . 540
Configurar GMSA en Windows Server 2016 o posterior . . . 542
Añada hosts e instale el plugin para Exchange . . . 543
Instale el plugin para Exchange desde el host del servidor de SnapCenter mediante cmdlets de PowerShell . . . 549
Instale el plugin de SnapCenter para Exchange silenciosamente desde la línea de comandos . . . 549
Supervise el estado de instalación del paquete de plugins de SnapCenter . . . 551
Configurar certificado de CA . . . 552
Configure SnapManager 7.x para Exchange y SnapCenter para que coexistan . . . 555
Instale el plugin de SnapCenter para VMware vSphere . . . 557
Implemente el certificado de CA . . . 557
Configure el archivo CRL . . . 557
Prepárese para la protección de datos . . . 557
Requisitos previos para usar el plugin de SnapCenter para Microsoft Exchange Server . . . 558
Uso de recursos, grupos de recursos y políticas para proteger un servidor de Exchange . . . 558
Realice backup de recursos de Exchange . . . 559
Flujo de trabajo de backup . . . 559
Verificación de la base de datos y el backup de Exchange . . . 560
Determine si hay recursos de Exchange disponibles para backup . . . 560
Crear políticas de backup para bases de datos de Exchange Server . . . 562
Crear grupos de recursos y añadir políticas para Exchange Server . . . 569
Cree una conexión de sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para Exchange Server . . . 572
Realizar backup de bases de datos de Exchange . . . 573
Realizar backup de grupos de recursos de Exchange . . . 578
Supervisar las operaciones de backup . . . 579
Cancelar las operaciones de backup de la base de datos de Exchange . . . 580
Consulte los backups de Exchange en la página Topology . . . 581
Restaurar recursos de Exchange . . . 583
Restaure el flujo de trabajo . . . 583
Requisitos para restaurar una base de datos de Exchange . . . 583
Restaurar bases de datos de Exchange . . . 584
Recuperación granular de correos y buzones de correo . . . 588
Restaurar una base de datos de servidor de Exchange desde un almacenamiento secundario . . . 588
Propagación de una réplica pasiva del nodo de Exchange . . . 589
Repropagación de una réplica mediante cmdlets de PowerShell para base de datos de Exchange . . . 590
Supervisar operaciones de restauración . . . 590
Cancelar las operaciones de restauración para base de datos de Exchange . . . 591
Proteger IBM DB2 . . . 593
Complemento de SnapCenter para IBM DB2 . . . 593
Información general sobre el plugin de SnapCenter para IBM DB2 . . . 593
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para IBM DB2 . . . 593
Funciones del plugin de SnapCenter para IBM DB2 . . . 594
Tipos de almacenamiento compatibles con el plugin de SnapCenter para IBM DB2 . . . 594

Privilegios mínimos de ONTAP requeridos para el plugin de IBM DB2 . . . 595
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para IBM DB2 . . . 598
Estrategia de backup para IBM DB2 . . . 598
Estrategia de restauración y recuperación para IBM DB2 . . . 601
Prepare la instalación del plugin de SnapCenter para IBM DB2 . . . 602
Flujo de trabajo de instalación del plugin de SnapCenter para IBM DB2 . . . 602
Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX . . . 602
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 608
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 609
Configure credenciales para el plugin de SnapCenter para IBM DB2 . . . 610
Configurar GMSA en Windows Server 2016 o posterior . . . 612
Instale el plugin de SnapCenter para IBM DB2 . . . 613
Configurar certificado de CA . . . 619
Prepárese para la protección de datos . . . 627
Requisitos previos para usar el plugin de SnapCenter para IBM DB2 . . . 627
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger IBM DB2 . . . 628
Realice un backup de los recursos de IBM DB2 . . . 628
Realice un backup de los recursos de IBM DB2 . . . 628
Detectar las bases de datos automáticamente . . . 630
Añada recursos manualmente al host del plugin . . . 630
Crear políticas de backup para IBM DB2 . . . 632
Crear grupos de recursos y añadir políticas . . . 634
Cree grupos de recursos y habilite la protección secundaria para recursos IBM DB2 en sistemas ASA R2 . . . 638
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para IBM DB2 . . . 641
Realizar un backup de las bases de datos de DB2 . . . 642
Realice un backup de los grupos de recursos . . . 649
Supervisar las operaciones de copia de seguridad de IBM DB2 . . . 650
Cancelar las operaciones de copia de seguridad de IBM DB2 . . . 651
Consulte los backups y los clones de IBM DB2 en la página Topology . . . 652
Restaurar IBM DB2 . . . 654
Restaure el flujo de trabajo . . . 654
Restaurar un backup de recursos añadido manualmente . . . 654
Restaurar y recuperar un backup de base de datos detectado automáticamente . . . 659
Supervisar las operaciones de restauración de IBM DB2 . . . 661
Clonar backups de recursos de IBM DB2 . . . 661
Flujo de trabajo de clonado . . . 661
Clonar un backup de IBM DB2 . . . 662
Supervisar las operaciones de clonación de IBM DB2 . . . 669
Divida un clon . . . 670
Elimine o divida clones de base de datos IBM DB2 después de actualizar SnapCenter . . . 671
Proteger PostgreSQL . . . 673
Complemento de SnapCenter para PostgreSQL . . . 673

Información general sobre el plugin de SnapCenter para PostgreSQL . . . 673
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para PostgreSQL . . . 673
Funciones del plugin de SnapCenter para PostgreSQL . . . 673
Tipos de almacenamiento compatibles con el plugin de SnapCenter para PostgreSQL . . . 674
Privilegios mínimos de ONTAP requeridos para el plugin de PostgreSQL . . . 675
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para PostgreSQL . . . 678
Estrategia de backup para PostgreSQL . . . 678
Estrategia de restauración y recuperación para PostgreSQL . . . 681
Prepare la instalación del plugin de SnapCenter para PostgreSQL . . . 682
Flujo de trabajo de instalación del plugin de SnapCenter para PostgreSQL . . . 682
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para PostgreSQL . . . 683
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 686
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 687
Configure credenciales para el plugin de SnapCenter para PostgreSQL . . . 688
Configurar GMSA en Windows Server 2016 o posterior . . . 690
Instale el plugin de SnapCenter para PostgreSQL . . . 691
Configurar certificado de CA . . . 697
Prepárese para la protección de datos . . . 705
Requisitos previos para usar el plugin de SnapCenter para PostgreSQL . . . 705
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger PostgreSQL . . . 706
Hacer backup de recursos de PostgreSQL . . . 706
Hacer backup de recursos de PostgreSQL . . . 706
Detecte los clústeres automáticamente . . . 708
Añada recursos manualmente al host del plugin . . . 708
Crear políticas de backup para PostgreSQL . . . 710
Crear grupos de recursos y añadir políticas . . . 713
Cree grupos de recursos y habilite la protección secundaria para recursos de PostgreSQL en sistemas R2 de ASA . . . 717
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para PostgreSQL . . . 720
Backup de PostgreSQL . . . 721
Realice un backup de los grupos de recursos . . . 727
Supervisar las operaciones de backup de PostgreSQL . . . 728
Cancelar las operaciones de backup para PostgreSQL . . . 729
Consulte los backups y los clones de PostgreSQL en la página Topology . . . 730
Restaurar PostgreSQL . . . 732
Restaure el flujo de trabajo . . . 732
Restaurar y recuperar un backup de recurso añadido manualmente . . . 732
Restaure y recupere un backup de clúster detectado automáticamente . . . 737
Restaurar recursos mediante los cmdlets de PowerShell . . . 740
Supervisar las operaciones de restauración de PostgreSQL . . . 742
Clonar backups de recursos de PostgreSQL . . . 743
Flujo de trabajo de clonado . . . 743
Clonar un backup de PostgreSQL . . . 744

Supervise las operaciones de clonación de PostgreSQL . . . 747
Divida un clon . . . 748
Elimine o divida clones de clústeres de PostgreSQL después de actualizar SnapCenter . . . 749
Proteger MySQL . . . 751
Complemento de SnapCenter para MySQL . . . 751
Información general sobre el plugin de SnapCenter para MySQL . . . 751
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para MySQL . . . 751
Funciones del plugin de SnapCenter para MySQL . . . 751
Tipos de almacenamiento compatibles con el plugin de SnapCenter para MySQL . . . 752
Privilegios mínimos de ONTAP requeridos para el plugin de MySQL . . . 753
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para MySQL 756
Estrategia de backup para MySQL . . . 756
Estrategia de restauración y recuperación para MySQL . . . 759
Prepare la instalación del plugin de SnapCenter para MySQL . . . 760
Flujo de trabajo de instalación del plugin de SnapCenter para MySQL . . . 760
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para MySQL . . . 760
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 764
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 765
Configure credenciales para el plugin de SnapCenter para MySQL . . . 766
Instale el plugin de SnapCenter para MySQL . . . 768
Configurar certificado de CA . . . 773
Prepárese para la protección de datos . . . 781
Requisitos previos para usar el plugin de SnapCenter para MySQL . . . 781
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger MySQL . . . 782
Realizar backup de recursos de MySQL . . . 782
Realizar backup de recursos de MySQL . . . 782
Detectar las bases de datos automáticamente . . . 784
Añada recursos manualmente al host del plugin . . . 784
Crear políticas de backup para MySQL . . . 785
Crear grupos de recursos y añadir políticas . . . 789
Cree grupos de recursos y habilite la protección secundaria para recursos de MySQL en sistemas R2 de ASA . . . 793
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para MySQL . . . 796
Hacer backup de MySQL . . . 797
Realice un backup de los grupos de recursos . . . 803
Supervisar las operaciones de backup de MySQL . . . 804
Cancelar las operaciones de backup para MySQL . . . 805
Consulte los backups y los clones de MySQL en la página Topology . . . 806
Restaure MySQL . . . 808
Restaure el flujo de trabajo . . . 808
Restaurar y recuperar un backup de recurso añadido manualmente . . . 808
Restaurar y recuperar un backup de base de datos detectado automáticamente . . . 813
Restaurar recursos mediante los cmdlets de PowerShell . . . 815
Supervise operaciones de restauración de MySQL . . . 817

Clonar backups de recursos de MySQL . . . 818
Flujo de trabajo de clonado . . . 818
Clonar un backup de MySQL . . . 819
Supervise las operaciones de clonación de MySQL . . . 822
Divida un clon . . . 823
Elimine o divida clones de base de datos MySQL después de actualizar SnapCenter . . . 824
Proteger aplicaciones mediante los complementos compatibles con NetApp . . . 826
Complementos compatibles con NetApp . . . 826
Información general sobre los plugins compatibles de NetApp . . . 826
Tareas que pueden llevarse a cabo con los plugins compatibles con NetApp . . . 826
Las funciones de los plugins compatibles con NetApp . . . 827
Tipos de almacenamiento admitidos por los plugins compatibles con NetApp . . . 828
Privilegios mínimos de ONTAP requeridos para el plugin compatible con NetApp . . . 828
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y de SnapVault para complementos compatibles con NetApp . . . 831
Defina una estrategia de backup . . . 831
La estrategia de backup para complementos compatibles con NetApp . . . 832
Tipos de estrategias de restauración compatibles con los recursos de plugins compatibles con NetApp añadidos manualmente . . . 833
Preparar la instalación de complementos compatibles con NetApp . . . 833
Flujo de trabajo de instalación de plugins compatibles con SnapCenter NetApp . . . 833
Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX . . . 834
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 838
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux y AIX . . . 839
Configure credenciales para plugins compatibles con NetApp . . . 840
Configurar GMSA en Windows Server 2016 o posterior . . . 842
Instale los complementos compatibles con NetApp . . . 844
Configurar certificado de CA . . . 850
Prepárese para la protección de datos . . . 858
Requisitos previos para usar los plugins compatibles de NetApp . . . 858
Cómo se usan los recursos, los grupos de recursos y las políticas para proteger los recursos de plugins compatibles con NetApp . . . 859
Realizar backup de los recursos de plugins compatibles con NetApp . . . 860
Realizar backup de los recursos de plugins compatibles con NetApp . . . 860
Añada recursos a los plugins compatibles con NetApp . . . 860
Crear políticas para los recursos de plugins compatibles con NetApp . . . 865
Crear grupos de recursos y añadir políticas . . . 869
Cree grupos de recursos y habilite la protección secundaria para los recursos en sistemas R2 de ASA 872
Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell . . . 875
Realizar backup de los recursos de plugins compatibles con NetApp individuales . . . 876
Realizar backup de grupos de recursos de plugins admitidos por NetApp . . . 881
Supervise operaciones de backup de recursos de plugins compatibles con NetApp . . . 882
Cancelar las operaciones de backup de los plugins compatibles con NetApp . . . 883
Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp en la página

Topology . . . 884
Restaurar recursos de plugins compatibles con NetApp . . . 886
Restaurar recursos de plugins admitidos por NetApp . . . 886
Restaurar un backup de recursos . . . 886
Supervise operaciones de restauración de recursos de plugins compatibles con NetApp . . . 890
Backups de recursos de plugins admitidos por Clone NetApp . . . 891
Backups de recursos de plugins admitidos por Clone NetApp . . . 891
Clonar desde un backup . . . 892
Supervisar operaciones de clonado de recursos de plugins admitidas por NetApp . . . 898
Proteja los sistemas de archivos Unix . . . 900
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para sistemas de archivos Unix . . . 900
Configuraciones admitidas . . . 900
Limitaciones . . . 901
Funciones . . . 901
Instale el plugin de SnapCenter para sistemas de archivos Unix . . . 901
Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux . . . 901
Añada hosts e instale el paquete de plugins para Linux mediante la interfaz gráfica de usuario . . . 903
Configure el servicio de cargador de plugins de SnapCenter . . . 906
Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux . . . 909
Habilite certificados de CA para plugins . . . 912
Instale el plugin de SnapCenter para VMware vSphere . . . 913
Implemente el certificado de CA . . . 913
Configure el archivo CRL . . . 913
Prepárese para la protección de sistemas de archivos Unix . . . 913
Hacer backup de sistemas de archivos Unix . . . 914
Descubra los sistemas de archivos UNIX disponibles para backup . . . 914
Crear directivas de backup para sistemas de archivos Unix . . . 914
Cree grupos de recursos y adjunte políticas para sistemas de archivos Unix . . . 917
Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Unix en sistemas ASA R2 . . . 919
Hacer backup de sistemas de archivos Unix . . . 922
Realizar un backup de los grupos de recursos de sistemas de archivos Unix . . . 923
Supervisar la copia de seguridad de sistemas de archivos Unix . . . 924
Vea los sistemas de archivos Unix protegidos en la página Topology . . . 925
Restaurar y recuperar sistemas de archivos Unix . . . 927
Restaurar sistemas de archivos Unix . . . 927
Supervisar las operaciones de restauración de sistemas de archivos Unix . . . 929
Clonar sistemas de archivos Unix . . . 930
Clonar backup de sistema de archivos Unix . . . 930
Divida un clon . . . 931
Supervisar operaciones de clonación de sistemas de archivos Unix . . . 932
Proteja las aplicaciones que se ejecutan en Azure NetApp Files . . . 934
Proteja las aplicaciones que se ejecutan en Azure NetApp Files . . . 934
Limitaciones . . . 934

Instale SnapCenter y cree las credenciales . . . 934
Instalar SnapCenter en la máquina virtual de Azure . . . 934
Cree las credenciales de Azure en SnapCenter . . . 936
Configure la cuenta de almacenamiento de Azure . . . 937
Cree la credencial para añadir el host del plugin . . . 937
Proteger las bases de datos SAP HANA . . . 938
Añadir hosts e instalar el plugin de SnapCenter para base de datos SAP HANA . . . 938
Añada una base de datos SAP HANA . . . 939
Crear políticas de backup para bases de datos SAP HANA . . . 939
Cree grupos de recursos y conecte políticas de backup de SAP HANA . . . 940
Realizar un backup de las bases de datos SAP HANA que se ejecutan en Azure NetApp Files . . . 941
Realice un backup de grupos de recursos SAP HANA . . . 942
Restaurar y recuperar bases de datos SAP HANA . . . 942
Clone el backup de base de datos SAP HANA . . . 943
Proteger bases de datos de Microsoft SQL Server . . . 945
Añadir hosts e instalar el plugin de SnapCenter para base de datos de SQL Server . . . 945
Crear políticas de backup para bases de datos de SQL Server . . . 945
Cree grupos de recursos y asocie las políticas de backup de SQL . . . 947
Realizar backups de bases de datos de SQL Server que se ejecutan en Azure NetApp Files . . . 948
Realizar un backup de grupos de recursos de SQL Server . . . 949
Restaurar y recuperar bases de datos de SQL Server . . . 949
Clone el backup de base de datos de SQL Server . . . 951
Proteger bases de datos de Oracle . . . 952
Añadir hosts e instalar el plugin de SnapCenter para base de datos de Oracle . . . 953
Crear políticas de backup para bases de datos de Oracle . . . 953
Crear grupos de recursos y asociar las políticas de backup de Oracle . . . 954
Realizar backups de las bases de datos de Oracle que se ejecutan en Azure NetApp Files . . . 955
Realice un backup de los grupos de recursos de Oracle . . . 956
Restaurar y recuperar bases de datos de Oracle . . . 956
Clone el backup de base de datos de Oracle . . . 959
Gestione SnapCenter Server y los plugins . . . 962
Consola de visualización . . . 962
Información general de la consola . . . 962
Cómo ver información en el panel . . . 966
Solicite informes de estado de trabajos desde la consola . . . 966
Solicite informes sobre el estado de protección desde el panel de control . . . 967
Gestione RBAC . . . 967
Modificar un rol . . . 967
Modificar usuarios y grupos . . . 968
Gestionar hosts . . . 968
Actualizar la información de la máquina virtual . . . 970
Modifique los hosts de plugins . . . 971
Inicie o reinicie servicios de plugin . . . 972
Suspender programaciones del mantenimiento del host . . . 972
Operaciones admitidas en la página Resources . . . 973

Gestionar políticas . . . 974
Modificar políticas . . . 974
Desvincular políticas . . . 975
Eliminar políticas . . . 975
Gestione grupos de recursos . . . 975
Detenga y reanude operaciones en grupos de recursos . . . 976
Eliminar grupos de recursos . . . 976
Gestionar backups . . . 977
Cambiar el nombre de los backups . . . 977
Eliminar backups . . . 977
Quitar la protección . . . 978
Eliminar clones . . . 978
Supervisar trabajos, programaciones, eventos y registros . . . 979
Supervisar trabajos . . . 979
Supervisar programaciones . . . 981
Supervisar eventos . . . 981
Supervisar registros . . . 981
Quite los trabajos y los registros de SnapCenter . . . 982
Información general sobre las funcionalidades de generación de informes de SnapCenter . . . 983
Acceder a informes . . . 984
Filtre su informe . . . 985
Exportar o imprimir informes . . . 985
Establezca el servidor SMTP para las notificaciones por correo electrónico . . . 985
Configure la opción para enviar informes por correo electrónico . . . 986
Gestione el repositorio del servidor SnapCenter . . . 986
Requisitos previos para proteger el repositorio de SnapCenter . . . 986
Realice un backup del repositorio de SnapCenter . . . 987
Ver los backups del repositorio de SnapCenter . . . 987
Restaurar el repositorio de la base de datos de SnapCenter . . . 987
Migre el repositorio de SnapCenter . . . 988
Restablecer la contraseña del repositorio de SnapCenter . . . 989
Gestione recursos de dominios que no son de confianza . . . 989
Modificar dominios que no son de confianza . . . 990
Cancele el registro de dominios de Active Directory que no son de confianza . . . 990
Gestione el sistema de almacenamiento . . . 991
Modifique la configuración del sistema de almacenamiento . . . 991
Elimine el sistema de almacenamiento . . . 993
Soporte PARA API REST . . . 994
Gestione la recogida de datos de EMS . . . 994
Detenga la recogida de datos de EMS . . . 995
Inicie la recogida de datos de EMS . . . 995
Cambie la programación de recogida de datos de EMS y SVM de destino . . . 995
Supervise el estado de recogida de datos de EMS . . . 995
Actualice el servidor de SnapCenter y los plugins . . . 997
Configure SnapCenter para la búsqueda de actualizaciones disponibles . . . 997

Actualizar el flujo de trabajo . . . 997
Rutas de actualización admitidas . . . 997
Actualice el servidor SnapCenter en el host de Windows . . . 998
Actualice el servidor SnapCenter en el host Linux . . . 1000
Actualizar los paquetes de complementos de SnapCenter . . . 1001
Actualización tecnológica . . . 1004
Actualización tecnológica del host de servidor de SnapCenter . . . 1004
Actualización tecnológica de un nodo en un clúster F5 . . . 1005
Desmantelamiento del antiguo host del servidor de SnapCenter . . . 1005
Realice una reversión al antiguo host del servidor de SnapCenter . . . 1005
Recuperación tras siniestros . . . 1005
Actualización tecnológica de los hosts de complementos de SnapCenter . . . 1007
Actualización tecnológica del sistema de almacenamiento . . . 1010
Actualice las copias de seguridad del almacenamiento primario . . . 1010
Actualice los backups del almacenamiento secundario . . . 1012
Desinstale SnapCenter Server y los plugins . . . 1014
Desinstale los paquetes de plugins de SnapCenter . . . 1014
Requisitos previos para quitar un host . . . 1014
Quitar un host . . . 1015
Desinstale plugins mediante la interfaz gráfica de usuario de SnapCenter . . . 1015
Desinstale los plugins de Windows mediante el cmdlet de PowerShell . . . 1016
Desinstale los plugins localmente en un host . . . 1017
Desinstale el paquete de plugins para Linux o AIX mediante la CLI . . . 1017
Desinstale el servidor SnapCenter en el host de Windows . . . 1018
Desinstale el servidor SnapCenter en el host Linux . . . 1018
Automatización mediante API de REST . . . 1020
Automatización de SnapCenter mediante API de REST . . . 1020
Cómo acceder a la API DE REST de SnapCenter de forma nativa . . . 1020
Base de servicios web DE REST . . . 1020
Recursos y representación estatal . . . 1020
Extremos de URI . . . 1021
Mensajes HTTP . . . 1021
Formato JSON . . . 1021
Características operativas básicas . . . 1021
Transacción de API de solicitud y respuesta . . . 1021
Compatibilidad con operaciones CRUD . . . 1022
Identificadores de objeto . . . 1022
Instancias y colecciones de objetos . . . 1022
Operaciones síncronas y asíncronas . . . 1022
Seguridad . . . 1023
Variables de entrada que controlan una solicitud API . . . 1023
Métodos HTTP . . . 1023
Solicitar encabezados . . . 1023
Solicitar el cuerpo . . . 1024
Filtrando objetos . . . 1024

Solicitando campos de objeto específicos . . . 1024
Ordenar objetos del conjunto de resultados . . . 1025
Paginación al recuperar objetos de una colección . . . 1025
Propiedades de tamaño . . . 1026
Interpretación de una respuesta API . . . 1026
Código de estado HTTP . . . 1027
Encabezados de respuesta . . . 1027
Cuerpo de respuesta . . . 1027
Errores . . . 1028
API DE REST compatibles con SnapCenter Server y los plugins . . . 1029
Autor . . . 1029
Dominios . . . 1029
Trabajos . . . 1029
Configuración . . . 1029
Hosts . . . 1030
Recursos . . . 1030
Completos . . . 1032
Clones . . . 1032
División de clones . . . 1032
Grupos de recursos . . . 1033
Normativas . . . 1033
Reducida . . . 1033
Share . . . 1034
Complementos . . . 1034
Leídos . . . 1035
Alertas . . . 1035
RBAC . . . 1035
Configuración . . . 1036
CertificadosConfiguración . . . 1036
Repositorio . . . 1036
Versión . . . 1036
Cómo acceder a las API de REST a través de la página web de API de Swagger . . . 1036
Comience con la API DE REST . . . 1037
Hola Mundo . . . 1037
Avisos legales . . . 1038
Derechos de autor . . . 1038
Marcas comerciales . . . 1038
Estadounidenses . . . 1038
Política de privacidad . . . 1038
Código abierto . . . 1038

Documentación de software SnapCenter

Notas de la versión

Notas de la versión

Obtenga información sobre las funciones nuevas y mejoradas disponibles en SnapCenter 6.2.

Para obtener una lista completa de las nuevas funciones y mejoras, consulte "Novedades de SnapCenter 6.2" .

Para obtener detalles sobre problemas conocidos, limitaciones, problemas solucionados y comandos nuevos y modificados, consulte la "Notas de la versión 6.2 del software SnapCenter" . Debe iniciar sesión con su cuenta de NetApp o crear una cuenta para acceder a las Notas de la versión.

Rutas de actualización admitidas para SnapCenter

La ruta de actualización muestra qué versiones de SnapCenter puede actualizar y qué versiones de complementos son compatibles.

Si actualiza SnapCenter Server a 6.2, actualice también los complementos a 6.2.

Si se encuentra en la versión de SnapCenter Server…	Puede actualizar directamente el servidor de SnapCenter a…	Versiones de plugins compatibles
6,0	6.0.1	• 6,0 • 6.0.1
	6,1	• 6,1
	6,2	• 6,2
6.0.1	6,1	• 6,1
	6,2	• 6,2
6,1	6,2	• 6,2

Para obtener información sobre cómo actualizar el plugin de SnapCenter para VMware vSphere, consulte "Actualice el plugin de SnapCenter para VMware vSphere".

Manos a la obra

Obtenga más información sobre el software SnapCenter

Información general de SnapCenter

El SnapCenter software es una plataforma simple, centralizada y escalable para la protección de datos consistente con todas las aplicaciones. Protege aplicaciones, bases de datos, sistemas de archivos de host y máquinas virtuales en sistemas ONTAP en la nube híbrida.

SnapCenter utiliza tecnologías NetApp Snapshot, SnapRestore, FlexClone, SnapMirror y SnapVault para proporcionar:

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

SnapCenter incluye SnapCenter Server y complementos livianos. Puede automatizar la implementación de complementos en hosts de aplicaciones remotas, programar operaciones de respaldo, verificación y clonación, y monitorear operaciones de protección de datos.

Puede instalar SnapCenter en sus instalaciones o en una nube pública para proteger los datos.

- En las instalaciones para proteger lo siguiente:
  - Datos en sistemas principales ONTAP FAS, AFF o ASA replicados a sistemas secundarios ONTAP FAS, AFF o ASA
  - Datos en sistemas principales ONTAP Select
  - Datos en sistemas principales y secundarios de ONTAP FAS, AFF o ASA, y protegidos en el almacenamiento de objetos local de StorageGRID
  - Datos en sistemas primarios y secundarios de ONTAP ASA R2
- Local en una nube híbrida para proteger lo siguiente:
  - Datos en sistemas principales ONTAP FAS, AFF o ASA replicados a Cloud Volumes ONTAP
  - Datos que se encuentran en sistemas primarios y secundarios de ONTAP FAS, AFF o ASA y están protegidos en el almacenamiento de objetos y archivos en la nube mediante la integración de respaldo y recuperación de NetApp
- En un cloud público para proteger lo siguiente:
  - Datos sobre sistemas principales de Cloud Volumes ONTAP (antes ONTAP Cloud)
  - Datos en Amazon FSX para ONTAP
  - Datos principales en Azure NetApp Files (Oracle, Microsoft SQL y SAP HANA)

Principales características

SnapCenter ofrece las siguientes funciones clave:

- Protección de datos centralizada y coherente con las aplicaciones de diferentes 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, IBM DB2, PostgreSQL, MySQL y sistemas de archivos host de Windows que se ejecutan en sistemas ONTAP. SnapCenter también admite la protección de aplicaciones como MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Backups basados en normativas

  Las copias de seguridad basadas en políticas aprovechan la tecnología Snapshot de NetApp para crear copias de seguridad basadas en disco, rápidas, eficientes en términos de espacio y consistentes con las aplicaciones. También puede configurar la protección automática de estas copias de seguridad en un almacenamiento secundario actualizando las relaciones de protección existentes.

- Copias de seguridad para múltiples recursos

  Puede realizar copias de seguridad de varios recursos (aplicaciones, bases de datos o sistemas de archivos de host) del mismo tipo a la vez utilizando los 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 una clonación rápida, que ahorra espacio y es consistente con las aplicaciones. Puede clonar en cualquier destino en la nube híbrida.

- Interfaz gráfica de usuario para la gestión de un solo usuario

  SnapCenter proporciona una única interfaz para administrar copias de seguridad y clones en cualquier destino de nube híbrida.

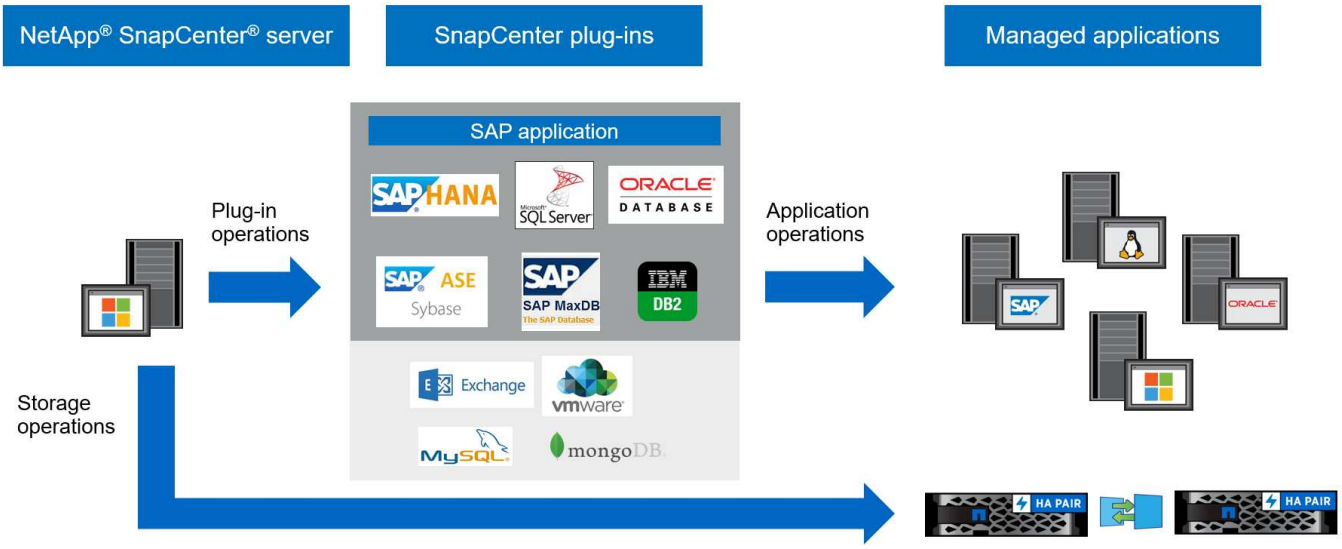
- API DE REST, cmdlets de Windows, comandos de UNIX

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

- Consola e informes centralizados para la protección de datos
- Control de acceso basado en roles (RBAC) para seguridad y delegación
- Una base de datos de repositorio incorporada con alta disponibilidad para almacenar todos los metadatos de backup
- Instalación mediante inserción automatizada de plug-ins
- Alta disponibilidad
- Recuperación ante desastres (DR)
- SnapLock "Más información"
- SnapMirror, sincronización activa (lanzado inicialmente como SnapMirror Business Continuity [SM-BC])
- Mirroring sincrónico "Más información"

Arquitectura y componentes de SnapCenter

SnapCenter utiliza un diseño en capas con un servidor de administración central y hosts de complementos. Los hosts del servidor y del complemento pueden estar en ubicaciones diferentes.



SnapCenter incluye el servidor de SnapCenter, el paquete de plugins de SnapCenter para Windows y el paquete de plugins de SnapCenter para Linux. Cada paquete contiene complementos para distintas aplicaciones y componentes de la infraestructura.

Servidor SnapCenter

El servidor SnapCenter es compatible con los sistemas operativos Microsoft Windows y Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). 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 almacena información sobre sus operaciones 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 de SnapCenter para Microsoft SQL Server	Paquete de plugins para Windows	Plugin para Windows	Host SQL Server	Windows
Complemento de SnapCenter para Windows	Paquete de plugins para Windows		Host Windows	Windows

Nombre de complemento	Incluido en el paquete de instalación	Requiere otros plugins	Instalado en el host	Plataforma compatible
Plugin de SnapCenter para Microsoft Exchange Server	Paquete de plugins para Windows	Plugin para Windows	Host Exchange Server	Windows
Plugin de SnapCentre para base de datos de Oracle	Paquete de plugins para Linux y el paquete de plugins para AIX	Complemento para UNIX	Host Oracle	Linux o AIX
Plugin de SnapCenter 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
Complemento de SnapCenter para IBM DB2	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	DB2 host	Linux, AIX o Windows
Complemento de SnapCenter para PostgreSQL	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host PostgreSQL	Linux o Windows
Plug-in de SnaoCenter para MySQL	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host MySQL	Linux o Windows
Plugin de SnapCenter para MongoDB	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host MongoDB	Linux o Windows
Complemento de SnapCenter para ORASCPM (Aplicaciones Oracle)	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host Oracle	Linux o Windows
Complemento de SnapCenter para SAP ASE	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host SAP	Linux o Windows

Nombre de complemento	Incluido en el paquete de instalación	Requiere otros plugins	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para SAP MaxDB	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host SAP MaxDB	Linux o Windows
Plugin de SnapCenter para plugin de almacenamiento	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host de almacenamiento	Linux o Windows

El SnapCenter Plug-in for VMware vSphere admite operaciones de copia de seguridad y restauración consistentes con fallas y con máquinas virtuales para máquinas virtuales (VM), almacenes de datos y discos de máquinas virtuales (VMDK). También admite operaciones de copia de seguridad y restauración consistentes con la aplicación para bases de datos y sistemas de archivos virtualizados.

Para proteger bases de datos, sistemas de archivos, máquinas virtuales o almacenes de datos en máquinas virtuales, implemente el SnapCenter Plug-in for VMware vSphere . Para obtener información, consulte "Documentación del plugin de SnapCenter para VMware vSphere" .

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 instalación de SnapCenter Server instala la base de datos del repositorio de MySQL Server de forma predeterminada. Si ya ha instalado MySQL Server y desea realizar una nueva instalación de SnapCenter Server, debe desinstalar MySQL Server.

SnapCenter admite MySQL Server 8.0.37 o posterior como base de datos del repositorio de SnapCenter . Si utiliza una versión anterior de MySQL Server con una versión anterior de SnapCenter, el proceso de actualización de SnapCenter actualiza MySQL Server a la versión 8.0.37 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 de SnapCenter

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).
- Compatible con algoritmos de seguridad que cumplen con el estándar de procesamiento de información federal (FIPS).
- Admite el uso de certificados de CA autorizados proporcionados por el cliente.
- Admite Seguridad de la capa de transporte (TLS) 1,3 para la comunicación con ONTAP. También puede usar TLS 1,2 para la comunicación entre clientes y servidores.
- Admite un determinado conjunto de conjuntos de conjuntos de cifrado SSL para proporcionar seguridad a través de la comunicación de red. "Leer más".
- 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.
- IPSec es compatible con SnapCenter en ONTAP para equipos host Windows y Linux. "Leer más".
- 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 intentos incorrectos de inicio de sesión.
- Admite la autenticación de certificados de CA entre SnapCenter Server y ONTAP. "Leer más".
- Se añade el verificador de integridad al servidor de SnapCenter y a los plugins y valida todos los binarios enviados durante las operaciones de instalación y actualización nuevas.

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 el certificado de CA para el plugin de SnapCenter para VMware vSphere. Para obtener más información, consulte "Crear e importar certificados".

Comunicación SSL bidireccional

La comunicación SSL bidireccional protege la comunicación mutua entre el servidor de SnapCenter y los plugins.

Descripción general de la autenticación basada en certificados

La autenticación basada en certificado verifica la autenticidad de los usuarios respectivos que intentan acceder al host del plugin de SnapCenter. El usuario debe exportar el certificado de servidor de SnapCenter sin clave privada e importarlo en el almacén de confianza del host del plugin. La autenticación basada en certificado solo funciona si la función SSL bidireccional está activada.

Autenticación multifactor (MFA)

La MFA usa un proveedor de identidades (IDP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de los usuarios. Esta funcionalidad mejora la seguridad de la autenticación al tener la opción de utilizar varios factores, como TOTP, biometría, notificaciones de inserción, etc. junto con el nombre de usuario y la contraseña existentes. Además, permite al cliente utilizar sus propios proveedores de identidades de usuario para obtener un inicio de sesión unificado (SSO) en toda su cartera.

La MFA solo se aplica a los inicios de sesión de la interfaz de usuario del servidor de SnapCenter. Los inicios de sesión se autentican a través de los servicios de Federación de Active Directory (AD FS) de IDP. Puede configurar varios factores de autenticación en AD FS. SnapCenter es el proveedor de servicios y debe configurar SnapCenter como parte de confianza en AD FS. Para habilitar la MFA en SnapCenter, necesitará los metadatos de AD FS.

Para obtener información sobre cómo habilitar la MFA, consulte "Active la autenticación multifactor".

Control de acceso basado en roles en SnapCenter

El control de acceso basado en roles (RBAC) de SnapCenter y los permisos de ONTAP permiten a los administradores de SnapCenter asignar acceso a recursos a usuarios o grupos. Este acceso administrado centralmente permite a los administradores de aplicaciones trabajar de forma segura dentro de entornos designados.

Debe crear o modificar roles y agregar acceso a recursos a los usuarios. Al configurar SnapCenter por primera vez, agregue usuarios o grupos de Active Directory a los roles y asigne recursos a esos usuarios o grupos.

> SnapCenter no crea cuentas de usuarios o grupos. Crear cuentas de usuario o grupo en el Directorio Activo del sistema operativo o de la base de datos.

Tipos de RBAC en SnapCenter

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

- RBAC de SnapCenter
- RBAC en el nivel de aplicaciones
- Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere
- Permisos de ONTAP

RBAC de SnapCenter

SnapCenter tiene roles predefinidos y usted puede asignar usuarios o grupos a estos roles.

- SnapCenter Admin
- App Backup and Clone Admin

- Backup and Clone Viewer
- Infrastructure Admin

Cuando se asigna un rol a un usuario, SnapCenter muestra los trabajos que son relevantes para ese usuario en la página Trabajos, a menos que el usuario tenga el rol SnapCenterAdmin.

También es posible crear nuevos roles y gestionar los permisos y los usuarios. 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.

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.

> Al crear un rol personalizado, asegúrese de que incluya todos los permisos del rol SnapCenterAdmin. Si copia solo algunos permisos, SnapCenter le impedirá realizar todas las operaciones.

Los usuarios deben autenticarse al iniciar sesión a través de la interfaz de usuario o los cmdlets de PowerShell. Si los usuarios tienen varios roles, seleccionan un rol después de iniciar sesión. También se requiere autenticación para ejecutar 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 realizar operaciones de protección de datos en un entorno de SQL Server, configure las credenciales de Windows o SQL correctas. Si desea realizar operaciones de protección de datos en un entorno de sistema de archivos de Windows en el almacenamiento ONTAP , el rol de administrador de SnapCenter debe tener privilegios de administrador en el host de Windows.

De manera similar, si desea realizar operaciones de protección de datos en una base de datos Oracle y si la autenticación del sistema operativo (SO) está deshabilitada en el host de la base de datos, debe configurar las credenciales con la base de datos Oracle o las credenciales de Oracle ASM. El servidor SnapCenter autentica las credenciales establecidas utilizando 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 VMware de SnapCenter es compatible con el control de acceso basado en roles de vCenter Server y de ONTAP. "Más información"

NOTA: NetApp recomienda crear una función de ONTAP para las operaciones del SnapCenter Plug-in for VMware vSphere y asignarle todos los privilegios necesarios.

Permisos de ONTAP

Debe crear una cuenta vsadmin con los permisos necesarios para acceder al sistema de almacenamiento."Más información"

Permisos asignados a los roles predefinidos de SnapCenter

Cuando agrega un usuario a un rol, asigne el permiso StorageConnection para habilitar la comunicación de la máquina virtual de almacenamiento (SVM) o asigne una SVM al usuario para otorgarle permiso para usar la SVM. El permiso de Conexión de almacenamiento permite a los usuarios crear conexiones SVM.

Por ejemplo, un administrador de SnapCenter puede crear conexiones SVM y asignarlas a usuarios administradores de App Backup y Clone, quienes no pueden crear ni editar conexiones SVM. Sin una conexión SVM, los usuarios no pueden realizar operaciones de copia de seguridad, clonación 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
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Backup and Clone Viewer

La función Visor de copias de seguridad y clones tiene una vista de solo lectura de todos los permisos. Esta función también tiene permisos habilitados para descubrimiento, informes y acceso al Panel de Control.

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

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Recurso	No	No	Sí	Sí	No
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
Protección secundaria	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

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
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	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
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Recuperación ante desastres en SnapCenter

La función de recuperación ante desastres (DR) de SnapCenter le permite recuperarse de desastres como la corrupción de recursos o fallos del servidor. Esto ayuda a restaurar el repositorio de SnapCenter, las programaciones del servidor, los componentes de configuración y el plugin de SnapCenter para SQL Server y su almacenamiento.

En esta sección se explican los dos tipos de DR que hay en SnapCenter:

Recuperación ante desastres de servidores SnapCenter

- Se realiza una copia de seguridad de los datos del servidor de SnapCenter y se pueden recuperar sin que se añada ningún plugin al servidor de SnapCenter ni se gestione.
- El servidor SnapCenter secundario debe instalarse en el mismo directorio de instalación y en el mismo puerto que el servidor SnapCenter primario.
- En el caso de la autenticación multifactor (MFA), durante la recuperación ante desastres del servidor de SnapCenter, cierre todas las pestañas del explorador y vuelva a abrir un explorador para iniciar sesión de nuevo. Esto borrará las cookies de sesión existentes o activas y actualizará los datos de configuración

correctos.

- La funcionalidad de recuperación ante desastres de SnapCenter utiliza la API de REST para realizar backups del servidor de SnapCenter. Consulte "Flujos de trabajo de API de REST para la recuperación ante desastres de SnapCenter Server".
- El archivo de configuración relacionado con la configuración de auditoría no se realiza un backup en el backup de recuperación ante desastres ni en el servidor de recuperación ante desastres después de la operación de restauración. Debe repetir manualmente la configuración del registro de auditoría.

Complemento SnapCenter y recuperación ante desastres de almacenamiento

La recuperación ante desastres solo está disponible para el plugin de SnapCenter para SQL Server. Si el plugin está inactivo, cambie a otro host de SQL y recupere los datos siguiendo unos pasos. Consulte "Recuperación ante desastres del plugin de SnapCenter para SQL Server".

SnapCenter usa ONTAP SnapMirror para replicar datos, que se pueden usar para la recuperación ante desastres manteniendo los datos sincronizados en un sitio secundario. Para iniciar la recuperación tras fallos, rompa la replicación de SnapMirror. Durante la conmutación de respaldo, invierta la sincronización para replicar los datos del sitio de recuperación de desastres de nuevo a la ubicación principal.

Licencias requeridas por 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	Requerido para FAS, AFF, ASA La licencia estándar de SnapCenter es una licencia basada en controladora y se incluye como parte de NetApp ONTAP One. 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, AFF o ASA, puede obtener una licencia de evaluación de NetApp ONTAP One poniéndose en contacto con el representante de ventas. Para obtener información sobre las licencias incluidas con NetApp ONTAP One, consulte "Licencias incluidas con NetApp ONTAP One" . 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
SnapMirror o SnapVault	ONTAP Se requieren licencias de SnapMirror o SnapVault si la replicación se habilita en SnapCenter.
SnapRestore	Necesario para restaurar y verificar backups. En sistemas de almacenamiento principales • Requerida en sistemas de destino de SnapVault para realizar la verificación remota y restaurar desde un backup • Requerida en sistemas de destino de SnapMirror para realizar la verificación remota
FlexClone	Necesario para clonar bases de datos y operaciones de verificación. En sistemas de almacenamiento principales y secundarios • Requerida en sistemas de destino de SnapVault para crear clones a partir de un backup de almacén secundario • Requerida en sistemas de destino de SnapMirror para crear clones a partir de un backup de SnapMirror secundario
Licencias de protocolos	• Licencia de iSCSI o FC para LUN • Licencia de CIFS para recursos compartidos de SMB • Licencia de NFS para VMDK de tipo NFS • Licencia de iSCSI o FC para VMDK de tipo VMFS Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible

Licencia	Donde se la requiere
Licencias estándar de SnapCenter (opcional)	Destinos secundarios 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.
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.

Las licencias avanzada y SnapCenter de servicios de archivos NAS de SnapCenter quedaron obsoletas y ya no están disponibles. La licencia estándar y la licencia basada en la capacidad ya no son necesarias para Amazon FSx para NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP y Azure NetApp Files.

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

SnapMirror sincronización activa en SnapCenter

La sincronización activa de SnapMirror permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo del sitio, lo que permite a las aplicaciones conmutar por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.

Para obtener más información sobre la sincronización activa de SnapMirror, consulte "Información general sobre sincronización activa de SnapMirror".

Para la sincronización activa de SnapMirror, asegúrese de haber cumplido los distintos requisitos de configuración de hardware, software y sistema. Para obtener más información, consulte "Requisitos previos"

Los plugins compatibles con esta función son el plugin de SnapCenter para SQL Server, el plugin de SnapCenter para Windows, el plugin de SnapCenter para base de datos de Oracle, el plugin de SnapCenter para base de datos SAP HANA, el plugin de SnapCenter para Microsoft Exchange Server y el plugin de SnapCenter para Unix.

Después de instalar SnapCenter Server y los complementos, debe habilitar la API REST para que SnapCenter detecte las relaciones de sincronización activas de SnapMirror .

- En el host del servidor SnapCenter , edite el archivo *C:\Program Files\ NetApp\SMCore\SMCoreServiceHost.dll.config* para modificar el valor del parámetro *IsRestEnabledForStorageConnection* a *true* y luego reinicie el servicio SnapCenter SMCore.
- En los hosts de complementos de Windows:
  - Edite el archivo *C:\Program Files\ NetApp\ SnapCenter\SMCore\SMCoreServiceHost.dll.config* para modificar el valor del parámetro *IsRestEnabledForStorageConnection* a *true*.
  - Edite el archivo *C:\Program Files\ NetApp\ SnapCenter\SMCore\SnapDriveService.dll.config* para modificar el valor del parámetro *IsRestEnabledForStorageConnection* a *true*.
  - Reinicie el servicio SnapCenter SMCore.

> Para admitir la proximidad del iniciador de host en SnapCenter, su valor, ya sea el origen o el destino deben establecerse en ONTAP.

Los casos de uso no compatibles con SnapCenter:

- Si convierte las cargas de trabajo asimétricas existentes de SnapMirror sincronización activa en simétricas cambiando la política de las relaciones de sincronización activa de SnapMirror de *automatedfailover* a *automatedfailoverduplex* en ONTAP, no se admite lo mismo en SnapCenter.
- Si existen backups de un grupo de recursos (ya protegido en SnapCenter) y se cambia la política de almacenamiento en las relaciones de sincronización activa de SnapMirror desde *automatedfailover* a *automatedfailoverduplex* en ONTAP, no se admite lo mismo en SnapCenter.

Conceptos clave de la protección de datos

Antes de usar SnapCenter, entienda conceptos clave para el backup, el clonado y la

restauración.

Recursos

Los recursos incluyen bases de datos, sistemas de archivos Windows o recursos compartidos de archivos incluidos en un backup o clonados con SnapCenter. En función del entorno, los recursos también pueden ser instancias de bases de datos, grupos de disponibilidad de SQL Server, bases de datos de Oracle, base de datos RAC o grupos de aplicaciones personalizados.

Grupo de recursos

Un grupo de recursos es una agrupacion de recursos en un host o un clúster, potencialmente de varios hosts y clústeres. Las operaciones realizadas en un grupo de recursos se aplican a todos sus recursos en función de la programación especificada. Puede ejecutar backups bajo demanda o programados para recursos o grupos individuales.

> Si un host de un grupo de recursos compartidos entra en modo de mantenimiento, todas las operaciones programadas de ese grupo se suspenden en todos los hosts.

Use plugins relevantes para realizar el backup de recursos específicos: Plugins de bases de datos para bases de datos, plugins del sistema de archivos para sistemas de archivos y plugin de SnapCenter para VMware vSphere para máquinas virtuales y almacenes de datos.

Normativas

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.

Se pueden seleccionar una o varias políticas al crear un grupo de recursos o al ejecutar un backup bajo demanda.

Un grupo de recursos define qué es necesario proteger y cuándo debe protegerse en términos de día y hora. Una política describe cómo se llevará a cabo la protección. Por ejemplo, si se necesita realizar un backup de todas las bases de datos o los sistemas de archivos de un host, puede crearse un grupo de recursos que incluya todas las bases de datos o los sistemas de archivos del host. Luego, se podrían vincular dos políticas al grupo de recursos: Una diaria y una horaria.

Al crear el grupo de recursos y añadir las políticas, es posible configurarlo para que se realice un backup completo todos los días, y agregar programaciones para backups de registros por hora.

Se pueden usar scripts previos y posteriores en operaciones de protección de datos. Estos scripts permiten la automatización antes o después del trabajo de protección de datos. Por ejemplo, un script podría notificar automáticamente cuando hay errores o advertencias en un trabajo de protección de datos. Comprender los requisitos para la creación de estos scripts es esencial antes de configurar scripts previos y posteriores.

Grupo de consistencia (GC)

Un grupo de consistencia es una colección de volúmenes administrados como una sola unidad. Los CG están sincronizados para garantizar la coherencia de los datos en todas las unidades de almacenamiento y volúmenes. En ONTAP, proporcionan una gestión sencilla y una garantía de protección para una carga de trabajo de aplicaciones que abarca múltiples volúmenes. Obtenga más información sobre "grupos de consistencia" .

Uso de scripts previos y posteriores

Los scripts previos y posteriores pueden automatizar las tareas de protección de datos antes o después del trabajo. Por ejemplo, puede agregar un script para notificarle los fallos o advertencias del trabajo. Antes de configurarlos, asegúrese de comprender los requisitos de estos scripts.

Tipos de scripts compatibles

Los siguientes tipos de scripts son compatibles con 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 tanto en sistemas de almacenamiento no virtualizados como en los virtualizados, se ejecutan en el host del plugin.

- Los scripts de Windows deben encontrarse en el host del plugin.

> La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

- Los scripts de UNIX deben encontrarse en el host del plugin.

> La ruta de acceso del script se valida en el momento de la ejecución.

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.

> No puede especificar varios scripts.

Tiempo de espera de scripts

De forma predeterminada, el tiempo de espera se establece 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.

Aplicaciones y sistemas de almacenamiento compatibles con SnapCenter

Debe conocer los sistemas de almacenamiento, aplicaciones y bases de datos que admite SnapCenter.

Sistemas de almacenamiento compatibles

- NetApp ONTAP 9.12.1 y versiones posteriores
- Azure NetApp Files
- Amazon FSX para ONTAP de NetApp

  Amazon FSx for NetApp ONTAP admite memoria no volátil express (NVMe) a través del Protocolo de control de transporte (TCP).

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

- Sistemas NetApp ASA r2 que ejecutan NetApp ONTAP 9.16.1 y versiones posteriores

  Debe utilizar ONTAP 9.17.1 si está utilizando SnapCenter Server 6.2 y los complementos de SnapCenter 6.2.

Aplicaciones y bases de datos compatibles

SnapCenter admite la protección de diferentes aplicaciones y bases de datos.

SnapCenter admite la protección de las cargas de trabajo de Oracle y Microsoft SQL en entornos de centro de datos definido por software (SDDC) de VMware Cloud on Amazon Web Services (AWS). "Más información".

Métodos de autenticación para las credenciales de SnapCenter

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 otro 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. Es necesario contar con credenciales de Windows para añadir hosts, instalar paquetes de plugins y programar trabajos.

Autenticación de dominio que no es de confianza

SnapCenter permite que los usuarios y grupos que pertenecen a dominios que no son de confianza creen credenciales de Windows. 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 los grupos y usuarios de grupos de trabajo locales no se produce durante la creación de las credenciales de Windows, pero se aplaza hasta que se realizan el registro del host y otras operaciones del 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 añadir una credencial de base de datos de Oracle, debe crear un usuario de Oracle en la base de datos de Oracle con Privileges de sysdba.

Autenticación de Oracle ASM

El método de autenticación de Oracle ASM autentica con una instancia de Oracle Automatic Storage Management (ASM). Si necesita acceder a una instancia de Oracle ASM y la autenticación del sistema operativo está deshabilitada en el host de base de datos, es necesaria la autenticación de Oracle ASM. Antes de agregar una credencial de Oracle ASM, cree un usuario oracle con SYSTEM Privileges 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.

Operaciones de SnapCenter compatibles con sistemas ASA r2

Los sistemas de almacenamiento ASA r2 son compatibles a partir de SnapCenter 6.1. "Obtenga más información sobre los sistemas R2 de ASA" .

SnapCenter admite la protección primaria y secundaria de aplicaciones que se ejecutan en sistemas físicos y en sistemas de archivos de máquinas virtuales (VMFS). SnapCenter utiliza API REST para todas las operaciones en sistemas ASA r2. Los sistemas ASA r2 no admiten ZAPI.

Operaciones compatibles con SnapCenter para sistemas ASA r2

- Creación de copias de seguridad primarias de aplicaciones
- Mover instantáneas del grupo de consistencia jerárquica al sistema de almacenamiento secundario
- Restaurar copias de seguridad de los sistemas de almacenamiento primario y secundario al host original o alternativo
  - Restauración en el lugar desde sistemas de almacenamiento primarios y secundarios mediante VMware vMotion
  - Conectar y copiar la restauración desde los sistemas de almacenamiento primario y secundario
- Clonación de las copias de seguridad en el host original o en el host alternativo
- Asignación de dispositivo sin formato (RDM)
- Protección de volúmenes de aplicaciones para Oracle
- Protección de SAP HANA NDV
- Vault
- Aprovisionamiento secundario del directorio de registro del host del complemento SQL

SnapCenter descubre o crea grupos de consistencia ONTAP . Configura relaciones SnapMirror en el clúster de destino para protección secundaria. "Obtenga más información sobre los grupos de consistencia de ONTAP" .

Después de actualizar a SnapCenter 6.2 (servidor y complementos) y ONTAP 9.17.1, SnapCenter cambia los grupos de consistencia planos a grupos de consistencia jerárquicos durante la primera copia de seguridad programada.

Para saber cómo habilitar la protección secundaria en los sistemas ASA r2 para su aplicación, consulte:

- "Habilitar la protección secundaria para los recursos de Microsoft SQL Server"
- "Habilitar la protección secundaria para los recursos de SAP HANA"
- "Habilitar la protección secundaria para los recursos de Oracle"
- "Habilitar la protección secundaria para los sistemas de archivos de Windows"
- "Habilitar la protección secundaria para los recursos de IBM Db2"
- "Habilitar la protección secundaria para los recursos de PostgreSQL"
- "Habilitar la protección secundaria para los recursos de MySQL"
- "Habilitar la protección secundaria para los sistemas de archivos Unix"

Operaciones no compatibles con SnapCenter para sistemas ASA r2

- Snapshots a prueba de manipulación
- Volúmenes de FlexGroup
- Migración de sistemas de almacenamiento ASA, AFF o FAS a sistemas de almacenamiento ASA r2
- Protección de bases de datos con una combinación de recursos ASA, AFF o FAS y recursos ASA r2
- Cambio de nombre de instantáneas
- Aprovisionamiento de recursos de Windows
- Protección secundaria si hay conmutación por error de sincronización activa de SnapMirror
- Protocolo de memoria no volátil express (NVMe) si la sincronización activa de SnapMirror está habilitada
- Protección de aplicaciones que se ejecutan en AIX
- Actualización tecnológica
- Recuperación ante desastres de recursos de Microsoft SQL

Inicio rápido para software SnapCenter

La guía de inicio rápido describe los pasos básicos para instalar y configurar el software SnapCenter.

1 **Prepárese para instalar el servidor SnapCenter**

Debe asegurarse de que se cumplen todos los requisitos para instalar el servidor SnapCenter.

- "Requisitos"
- "Regístrese para acceder al software SnapCenter"
- "Habilite la autenticación multifactor"

2 **Instale el servidor SnapCenter**

El servidor SnapCenter puede instalarse en hosts de Windows o Linux. Descargue el paquete de instalación del servidor de SnapCenter desde "Sitio de soporte de NetApp" y ejecute el instalador.

- "Instale el servidor SnapCenter en Windows"
- "Instale el servidor SnapCenter en Linux"

3 **Configurar el servidor SnapCenter**

Después de instalar el servidor SnapCenter, debe configurarlo según su entorno.

4 **Instale el plugin para la aplicación**

Asegúrese de que se cumplen todos los requisitos para la instalación del plugin específico de la aplicación en función de la aplicación en uso y, a continuación, continúe con la instalación del plugin correspondiente.

Proteja su aplicación

Después de instalar correctamente el servidor de SnapCenter y los plugins necesarios, es posible iniciar la creación de backups de aplicaciones. Más adelante, estos backups se podrán utilizar para fines de restauración y clonado cuando sea necesario.

Instalar y configurar SnapCenter Server

Prepare la instalación del servidor SnapCenter

Requisitos para instalar el servidor SnapCenter

Antes de instalar SnapCenter Server en el host de Windows o Linux, debe revisar y asegurarse de que se cumplan todos los requisitos para su entorno.

Requisitos del dominio y grupos de trabajo para el host Windows

El servidor de SnapCenter puede instalarse en un host de Windows que esté en un dominio o en un grupo de trabajo.

El usuario que tiene Privileges de administrador puede instalar el servidor de SnapCenter.

- 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

Debería estar familiarizado con los requisitos de espacio y tamaño.

Elemento	Requisitos del host de Windows	Requisitos del host Linux
Sistemas operativos	Microsoft Windows Solo se admiten las versiones en inglés, alemán, japonés y chino simplificado de los sistemas operativos. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".	• Red Hat Enterprise Linux (RHEL) 8 y 9 • SUSE Linux Enterprise Server (SLES) 15 Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".
Recuento de CPU mínimo	4 núcleos	4 núcleos

Elemento	Requisitos del host de Windows	Requisitos del host Linux
RAM mínimo	8 GB El grupo de buffers de MySQL Server utiliza el 20 por ciento de la RAM total.	8 GB
Espacio mínimo en disco duro para el software y los registros del servidor SnapCenter	7 GB Si tiene el repositorio de SnapCenter en la misma unidad donde está instalado el servidor SnapCenter, se recomienda tener 15 GB.	15 GB
Espacio en disco duro mínimo para el repositorio de SnapCenter	8 GB NOTA: Si tiene el servidor SnapCenter en la misma unidad en la que está instalado el repositorio de SnapCenter, se recomienda tener 15 GB.	No aplicable

Elemento	Requisitos del host de Windows	Requisitos del host Linux
Paquetes de software obligatorios	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell 7.4.2 o posterior Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla para sistemas heredados que no tienen conectividad a Internet".	• .NET Framework 8.0.12 (y todos los parches 8,0.x posteriores) • PowerShell 7.4.2 o posterior • Nginx es un servidor web que se puede utilizar como proxy inverso • PAM-devel PAM (Pluggable Authentication Modules) es una herramienta de seguridad del sistema que permite a los administradores del sistema establecer la política de autenticación sin tener que volver a compilar programas que hacen autenticación.

El núcleo ASP.NET necesita IIS_IUSRS para acceder al sistema de archivos temporales en el servidor SnapCenter en Windows.

Requisitos del host SAN

SnapCenter no incluye utilidades de host ni un DSM. Si el host de SnapCenter forma parte de un entorno SAN (FC/iSCSI), puede que tenga que instalar y configurar software adicional en el host de SnapCenter.

- Utilidades de host: Las utilidades de host son compatibles con FC e iSCSI, y le permiten usar MPIO en sus servidores Windows. "Más información".
- 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".

Requisitos de navegador

El software SnapCenter es compatible con Chrome 125 y versiones posteriores, y Microsoft Edge 110.0.1587.17 y versiones posteriores.

Requisitos de puertos

El software SnapCenter requiere diferentes puertos para la comunicación entre diferentes componentes.

- Las aplicaciones no pueden compartir los puertos.
- En el caso de los puertos personalizables, puede seleccionar un puerto personalizado durante la

instalación si no quiere usar el predeterminado.

- 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.

Nombre de puerto	Números de puerto	Protocolo	Dirección	Descripción
Puerto web de SnapCenter	8146	HTTPS	Bidireccional	Este puerto se usa para establecer la comunicación entre el cliente SnapCenter (el usuario SnapCenter) y el servidor SnapCenter, y también se utiliza para establecer la comunicación de los hosts del plugin con el servidor SnapCenter. Puede personalizar el número de puerto.
Puerto de comunicación SMCore de SnapCenter	8145	HTTPS	Bidireccional	Este puerto se utiliza para establecer la comunicación entre SnapCenter Server y los hosts en los que se han instalado los plugins de SnapCenter. Puede personalizar el número de puerto.

Nombre de puerto	Números de puerto	Protocolo	Dirección	Descripción
Puerto de servicio del programador	8154	HTTPS		Este puerto se utiliza para orquestar los flujos de trabajo del programador de SnapCenter para todos los plugins gestionados dentro del host del servidor SnapCenter de forma centralizada. Puede personalizar el número de puerto.
Puerto RabbitMQ	5672	TCP		Este es el puerto predeterminado en el que RabbitMQ escucha y se utiliza para la comunicación del modelo editor-suscriptor entre el servicio Programador y SnapCenter.
Puerto MySQL	3306	HTTPS		El puerto se utiliza para comunicarse con la base de datos del repositorio de SnapCenter. Puede crear conexiones seguras desde el servidor SnapCenter al servidor MySQL. "Leer más"

Nombre de puerto	Números de puerto	Protocolo	Dirección	Descripción
Hosts de plugins de Windows	135, 445	TCP		Este puerto se utiliza para establecer la comunicación entre el servidor de SnapCenter y el host en el que se está instalando el plugin. El rango de puertos dinámicos adicional especificado por Microsoft también debe estar abierto.
Hosts de plugins de Linux o AIX	22	SSH	Unidireccional	Este puerto se utiliza para establecer la comunicación entre el servidor de SnapCenter y el host, iniciado desde el servidor al host del cliente.
Paquete de plugins de SnapCenter para Windows, Linux o AIX	8145	HTTPS	Bidireccional	Este puerto se utiliza para establecer la comunicación entre SMCore y los hosts en los que está instalado el paquete de plugins. Personalizable. Puede personalizar el número de puerto.
Plugin de SnapCenter para base de datos de Oracle	27216			El puerto de JDBC predeterminado, lo utiliza el plugin para Oracle para conectarse a la base de datos de Oracle.

Nombre de puerto	Números de puerto	Protocolo	Dirección	Descripción
Plugin de SnapCenter para base de datos de Exchange	909			NET predeterminado. El plugin para Windows utiliza el puerto TCP para conectarse a las devoluciones de llamadas VSS de Exchange.
Complementos compatibles con NetApp para SnapCenter	9090	HTTPS		Este es un puerto interno que se utiliza solo en el host del complemento; no se requiere excepción de firewall. La comunicación entre el servidor SnapCenter y los complementos se enruta a través del puerto 8145.
Puerto de comunicación del clúster de ONTAP o de SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidireccional	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.

Nombre de puerto	Números de puerto	Protocolo	Dirección	Descripción
Plugin de SnapCenter para base de datos SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidireccional	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. Puede personalizar el número de puerto.
Complemento de SnapCenter para PostgreSQL	5432			Este puerto es el puerto PostgreSQL predeterminado utilizado para la comunicación del plugin para PostgreSQL con el clúster PostgreSQL. Puede personalizar el número de puerto.

Regístrese para acceder al software de SnapCenter

Debe registrarse para acceder al software de SnapCenter si es nuevo en Amazon FSx for NetApp ONTAP o Azure NetApp Files y no tiene una cuenta de NetApp existente.

Antes de empezar

- Debe tener acceso al ID de correo electrónico corporativo.
- Si utiliza Azure NetApp Files, debe tener el ID de suscripción de Azure.
- Si está utilizando Amazon FSx para NetApp ONTAP, debe tener el ID del sistema de archivos de su sistema de archivos FSx para ONTAP.

Acerca de esta tarea

Su registro está sujeto a validaciones de información y puede tardar hasta un día en confirmar y actualizar la nueva cuenta del sitio de soporte de NetApp (NSS) a acceso **completo** desde el acceso **guest**.

Pasos

1. Haga clic https://mysupport.netapp.com/site/user/registration para registrarse.
2. Ingrese su ID de correo electrónico corporativo, complete el captcha, acepte la política de privacidad de NetApp y haga clic en **Enviar**.
3. Autentique el registro ingresando el OTP enviado a su ID de correo electrónico y haga clic en **Continuar**.
4. En la página de finalización del registro, introduzca los siguientes detalles para completar el registro.

a. Seleccione **Cliente NetApp / Usuario final**.

b. En el campo NÚMERO DE SERIE, introduzca el ID de suscripción de Azure si utiliza Azure NetApp Files o el ID del sistema de archivos si utiliza Amazon FSx para NetApp ONTAP.

Puede emitir un ticket en https://mysupport.netapp.com/site/help si se enfrenta a cualquier problema durante el registro o para saber el estado.

Autenticación multifactor (MFA)

Gestionar la autenticación multifactor (MFA)

Puede administrar la funcionalidad de autenticación multifactor (MFA) en el servidor del servicio de federación de Active Directory (AD FS) y el servidor SnapCenter.

Habilitar la autenticación multifactor (MFA)

Puede habilitar la funcionalidad MFA para SnapCenter Server con los comandos de PowerShell.

Acerca de esta tarea

- SnapCenter admite inicios de sesión basados en SSO cuando otras aplicaciones están configuradas en el mismo AD FS. En determinadas configuraciones de AD FS, SnapCenter puede requerir autenticación de usuario por motivos de seguridad, dependiendo de la persistencia de la sesión de AD FS.
- La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también se puede ver "Guía de referencia de cmdlets de SnapCenter Software".

Antes de empezar

- El servicio de Federación de Active Directory de Windows (AD FS) debe estar activo y en ejecución en el dominio correspondiente.
- Debe tener un servicio de autenticación multifactor compatible con AD FS, como Azure MFA, Cisco Duo, etc.
- La Marca de hora del servidor SnapCenter y AD FS debe ser la misma independientemente de la zona horaria.
- Adquirir y configurar el certificado de CA autorizado para SnapCenter Server.

  El certificado DE CA es obligatorio por los siguientes motivos:

  - Garantiza que las comunicaciones ADFS-F5 no se interrumpan porque los certificados autofirmados son únicos en el nivel de nodo.
  - Garantiza que durante la actualización, reparación o recuperación ante desastres en una configuración independiente o de alta disponibilidad, el certificado autofirmado no se vuelva a crear, con lo que se evita la reconfiguración de la MFA.
  - Garantiza resoluciones IP-FQDN.

    Para obtener información sobre el certificado de CA, consulte "Genere un archivo CSR de certificado de CA".

Pasos

1. Conéctese al host de Servicios de Federación de Active Directory (AD FS).

2. Descargue el archivo de metadatos de la federación de AD FS desde "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml.
3. Copie el archivo descargado en el servidor SnapCenter para habilitar la función MFA.
4. Inicie sesión en SnapCenter Server como usuario administrador de SnapCenter mediante PowerShell.
5. Con la sesión de PowerShell, genere el archivo de metadatos MFA de SnapCenter mediante el cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   El parámetro path especifica la ruta al guardar el archivo de metadatos de MFA en el host del servidor de SnapCenter.

6. Copie el archivo generado en el host AD FS para configurar SnapCenter como entidad cliente.
7. Habilite la MFA para el servidor de SnapCenter mediante el `Set-SmMultiFactorAuthentication` cmdlet.
8. (Opcional) Compruebe el estado y la configuración de MFA mediante `Get-SmMultiFactorAuthentication` cmdlet.
9. Vaya a la consola de administración de Microsoft (MMC) y realice los pasos siguientes:
   a. Haga clic en **Archivo** > **Agregar o quitar Snapin**.
   b. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
   c. En la ventana del complemento certificados, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
   d. Haga clic en **raíz de consola** > **certificados – Equipo local** > **personal** > **certificados**.
   e. Haga clic con el botón derecho del ratón en el certificado de CA vinculado a SnapCenter y, a continuación, seleccione **todas las tareas** > **Administrar claves privadas**.
   f. En el asistente de permisos, realice los siguientes pasos:
      i. Haga clic en **Agregar**.
      ii. Haga clic en **Ubicaciones** y seleccione el host en cuestión (parte superior de la jerarquía).
      iii. Haga clic en **Aceptar** en la ventana emergente **Ubicaciones**.
      iv. En el campo de nombre de objeto, introduzca 'IIS_IUSRS' y haga clic en **comprobar nombres** y haga clic en **Aceptar**.

      Si la comprobación se realiza correctamente, haga clic en **Aceptar**.

10. En el host AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
    a. Haga clic con el botón derecho del ratón en **Fideicomiso del Partido** > **Agregar confianza del Partido** > **Inicio**.
    b. Seleccione la segunda opción y examine el archivo de metadatos de MFA de SnapCenter y haga clic en **Siguiente**.
    c. Especifique un nombre para mostrar y haga clic en **Siguiente**.
    d. Elija una política de control de acceso según sea necesario y haga clic en **Siguiente**.
    e. Seleccione la configuración en la siguiente ficha para Predeterminado.
    f. Haga clic en **Finalizar**.

    SnapCenter se refleja ahora como una parte que confía en el nombre para mostrar proporcionado.

11. Seleccione el nombre y realice los siguientes pasos:
    a. Haga clic en **Editar directiva de emisión de reclamaciones**.
    b. Haga clic en **Agregar regla** y haga clic en **Siguiente**.
    c. Especifique un nombre para la regla de reclamación.
    d. Seleccione **Active Directory** como almacén de atributos.
    e. Seleccione el atributo como **Nombre-principal-usuario** y el tipo de reclamación saliente como **Nombre-ID**.
    f. Haga clic en **Finalizar**.
12. Ejecute los siguientes comandos de PowerShell en el servidor ADFS.

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

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

13. Realice los siguientes pasos para confirmar que los metadatos se han importado correctamente.
    a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía y seleccione **Propiedades**.
    b. Asegúrese de que se rellenan los campos puntos finales, identificadores y firma.
14. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

La funcionalidad MFA de SnapCenter también se puede habilitar usando las API de REST.

Para obtener información sobre la solución de problemas, consulte "Los intentos de inicio de sesión simultáneos en varias pestañas muestran un error MFA".

Actualizar metadatos de MFA de AD FS

Debe actualizar los metadatos de la MFA de AD FS en SnapCenter cada vez que haya alguna modificación en el servidor de AD FS, como la actualización, la renovación de certificados de CA, la recuperación ante desastres, etc.

Pasos

1. Descargue el archivo de metadatos de la federación de AD FS desde "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copie el archivo descargado en el servidor SnapCenter para actualizar la configuración de MFA.
3. Actualice los metadatos de AD FS en SnapCenter ejecutando el siguiente cmdlet:

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

4. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Actualice los metadatos de MFA de SnapCenter

Debe actualizar los metadatos del MFA de SnapCenter en AD FS cada vez que haya alguna modificación en el servidor ADFS como, por ejemplo, la reparación, la renovación de certificados de CA, la recuperación ante

desastres, etc.

Pasos

1. En el host AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
   a. Seleccione **Confiando Fideicomisos de Partes**.
   b. Haga clic con el botón derecho en la confianza de la parte de confianza que se creó para SnapCenter y seleccione * Eliminar *.

      Se mostrará el nombre definido por el usuario de la confianza de la parte que confía.

   c. Habilite la autenticación multifactor (MFA).

      Consulte "Active la autenticación multifactor".

2. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Deshabilitar la autenticación multifactor (MFA)

Pasos

1. Deshabilite la MFA y borre los archivos de configuración que se crearon cuando se habilitó MFA con el `Set-SmMultiFactorAuthentication` cmdlet.
2. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Gestione la autenticación multifactor (MFA) con la API de REST, PowerShell y SCCLI

El inicio de sesión de MFA es compatible con el explorador, la API de REST, PowerShell y SCCLI. MFA es compatible a través de un gestor de identidades de AD FS. Puede habilitar MFA, deshabilitar MFA y configurar MFA desde la GUI, la API de REST, PowerShell y SCCLI.

Configure AD FS como OAuth/OIDC

- Configurar AD FS usando el asistente de la GUI de Windows*
  1. Vaya a **Server Manager Dashboard** > **Tools** > **ADFS Management**.
  2. Vaya a **ADFS** > **Grupos de aplicaciones**.
     a. Haga clic con el botón derecho en **Grupos de aplicaciones**.
     b. Seleccione **Agregar grupo de aplicaciones** e introduzca **Nombre de la aplicación**.
     c. Seleccione **Aplicación de servidor**.
     d. Haga clic en **Siguiente**.
  3. Copiar **Identificador de Cliente**.

     Este es el ID de cliente.
     .. Agregar URL de devolución de llamada (URL del servidor de SnapCenter) en URL de redireccionamiento.
     .. Haga clic en **Siguiente**.

  4. Selecciona **Generar secreto compartido**.

Copie el valor secreto. Este es el secreto del cliente.
.. Haga clic en **Siguiente**.

5. En la página **Resumen**, haz clic en **Siguiente**.
   a. En la página **Completo**, haz clic en **Cerrar**.
6. Haga clic con el botón derecho en el recién agregado **Grupo de aplicaciones** y seleccione **Propiedades**.
7. Seleccione **Añadir aplicación** en Propiedades de la aplicación.
8. Haga clic en **Añadir aplicación**.

   Seleccione Web API y haga clic en **Siguiente**.

9. En la página Configurar API Web, introduzca la URL del servidor SnapCenter y el identificador de cliente creados en el paso anterior en la sección Identificador.
   a. Haga clic en **Agregar**.
   b. Haga clic en **Siguiente**.
10. En la página **Elegir Política de Control de Acceso**, selecciona la política de control en función de tus requisitos (por ejemplo, Permitir a todos y requerir MFA) y haz clic en **Siguiente**.
11. En la página **Configurar permiso de aplicación**, por defecto se selecciona openid como un ámbito, haga clic en **Siguiente**.
12. En la página **Resumen**, haz clic en **Siguiente**.

    En la página **Completo**, haz clic en **Cerrar**.

13. En la página **Sample Application Properties**, haz clic en **OK**.
14. Token JWT emitido por un servidor de autorización (AD FS) y destinado a ser consumido por el recurso.

    La reclamación 'aud' o de público de este token debe coincidir con el identificador del recurso o la API web.

15. Edite la WebAPI seleccionada y compruebe que la URL de devolución de llamada (URL del servidor de SnapCenter) y el identificador de cliente se han agregado correctamente.

    Configure OpenID Connect para proporcionar un nombre de usuario como reclamaciones.

16. Abra la herramienta **AD FS Management** ubicada en el menú **Tools** en la parte superior derecha del Administrador del servidor.
    a. Seleccione la carpeta **Grupos de aplicaciones** en la barra lateral izquierda.
    b. Seleccione la API web y haga clic en **EDITAR**.
    c. Vaya a la pestaña Reglas de transformación de emisión
17. Haga clic en **Agregar regla**.
    a. Seleccione el **Enviar atributos LDAP como reclamaciones** en el menú desplegable de la plantilla de regla de reclamación.
    b. Haga clic en **Siguiente**.
18. Introduzca el nombre de la regla de reclamación *.

a. Seleccione **Active Directory** en el menú desplegable del almacén de atributos.
b. Seleccione **User-Principal-Name** en el menú desplegable **LDAP Attribute** y **UPN** en el menú desplegable O*utgoing Claim Type*.
c. Haga clic en **Finalizar**.

Crear grupo de aplicaciones con comandos de PowerShell

Puede crear el grupo de aplicaciones, la API web y agregar el alcance y las reclamaciones mediante comandos de PowerShell. Estos comandos están disponibles en formato de script automatizado. Para obtener más información, consulte <link to KB article>.

1. Cree el nuevo grupo de aplicaciones en AD FS mediante el siguiente comamnd.

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

   `ClientRoleIdentifier` nombre del grupo de aplicaciones

   `redirectURL` URL válida para redirección después de la autorización

2. Cree la aplicación de servidor de AD FS y genere el secreto de cliente.

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

3. Cree la aplicación API Web de ADFS y configure el nombre de política que debe utilizar.

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

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

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

4. Obtenga el ID de cliente y el secreto de cliente del resultado de los siguientes comandos, porque solo se muestra una vez.

   ```
   "client_id = $identifier"

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

5. Otorgue a la aplicación AD FS los permisos allatclaims y openid.

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

   $transformrule = @"

   @RuleTemplate = "LdapClaims"

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

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

"AD AUTHORITY"]

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

"@
```

6. Escriba el archivo de reglas de transformación.

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

7. Asigne un nombre a la aplicación Web API y defina sus reglas de transformación de emisión mediante un archivo externo.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Actualizar tiempo de caducidad del token de acceso

Puede actualizar el tiempo de caducidad del token de acceso mediante el comando PowerShell.

Acerca de esta tarea

- Un token de acceso solo se puede utilizar para una combinación específica de usuario, cliente y recurso. Los tokens de acceso no se pueden revocar y son válidos hasta su vencimiento.
- De forma predeterminada, el tiempo de caducidad de un token de acceso es de 60 minutos. Este tiempo de caducidad mínimo es suficiente y se escala. Debe proporcionar el valor suficiente para evitar trabajos críticos para el negocio en curso.

Paso

Para actualizar el tiempo de caducidad del token de acceso para un grupo de aplicaciones WEBAPI, utilice el siguiente comando en el servidor AD FS.

+

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

Obtenga el token portador de AD FS

Debe rellenar los parámetros mencionados a continuación en cualquier cliente REST (como Postman) y le pedirá que rellene las credenciales de usuario. Además, debe introducir la autenticación de segundo factor (algo que tiene y algo que es) para obtener el token de portador.

+
La validez del token portador se puede configurar desde el servidor de AD FS por aplicación y el período de validez predeterminado es de 60 minutos.

Campo	Valor
Tipo de concesión	Código de autorización
URL de devolución de llamada	Introduzca la URL base de la aplicación si no tiene una URL de devolución de llamada.
URL de autenticación	[adfs-domain-name]/adfs/oauth2/authorized
URL de token de acceso	[adfs-domain-name]/adfs/oauth2/token
ID del cliente	Introduzca el ID de cliente de AD FS
Secreto de cliente	Introduzca el secreto de cliente de AD FS
Ámbito	ID de código abierto
Autenticación de cliente	Enviar como cabecera de AUTENTICACIÓN básica
Recurso	En la pestaña **Opciones avanzadas**, agregue el campo Recurso con el mismo valor que la URL de devolución de llamada, que viene como un valor “aud” en el token JWT.

Configure MFA en SnapCenter Server mediante PowerShell, SCCLI y la API de REST

Es posible configurar la MFA en SnapCenter Server mediante PowerShell, SCCLI y la API DE REST.

Autenticación CLI MFA de SnapCenter

En PowerShell y SCCLI, el cmdlet existente (Open-SmConnection) se amplía con un campo más llamado “AccessToken” para utilizar el token portador para autenticar al usuario.

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

Una vez ejecutado el cmdlet anterior, se crea una sesión para que el usuario respectivo ejecute más cmdlets de SnapCenter.

Autenticación de la API de REST MFA de SnapCenter

Use el token portador en el formato *Authorization=Bearer <access token>* en el cliente de la API REST (como Postman o Swagger) y mencione el nombre de rol del usuario en el encabezado para obtener una respuesta exitosa de SnapCenter.

Flujo de trabajo de la API de REST de MFA

Cuando MFA se configura con AD FS, debe autenticarse mediante un token de acceso (portador) para acceder a la aplicación SnapCenter mediante cualquier API REST.

Acerca de esta tarea

- Puede utilizar cualquier cliente de REST, como Postman, Swagger UI o FireCamp.
- Obtenga un token de acceso y utilícelo para autenticar las solicitudes posteriores (API de REST de SnapCenter) para realizar cualquier operación.
- Pasos*

Para autenticarse a través de AD FS MFA

1. Configure el cliente REST para que llame al punto final de AD FS para obtener el token de acceso.

   Cuando pulse el botón para obtener un token de acceso para una aplicación, se le redirigirá a la página SSO de AD FS, donde debe proporcionar sus credenciales de AD y autenticarse con MFA.
   1. En la página SSO de AD FS, escriba su nombre de usuario o correo electrónico en el cuadro de texto Nombre de usuario.

   +
   Los nombres de usuario deben formatearse como usuario@dominio o dominio\usuario.

2. En el cuadro de texto Contraseña, escriba la contraseña.
3. Haga clic en **Iniciar sesión**.
4. En la sección **Opciones de inicio de sesión**, selecciona una opción de autenticación y autentica (dependiendo de tu configuración).
   - Push: Aprueba la notificación push que se envía al teléfono.
   - Código QR: Utilice la aplicación móvil AUTH Point para escanear el código QR y, a continuación, escriba el código de verificación que se muestra en la aplicación
   - Contraseña de un solo uso: Escriba la contraseña de un solo uso para el token.
5. Después de la autenticación correcta, se abrirá una ventana emergente que contiene el acceso, el ID y el token de refrescamiento.

   Copie el token de acceso y utilícelo en la API de REST de SnapCenter para realizar la operación.

6. En la API de REST, debe pasar el token de acceso y el nombre de rol en la sección de encabezado.
7. SnapCenter valida este token de acceso desde AD FS.

   Si es un token válido, SnapCenter lo decodifica y obtiene el nombre de usuario.

8. Con el nombre de usuario y el nombre de rol, SnapCenter autentica al usuario para ejecutar la API.

   Si la autenticación se realiza correctamente, SnapCenter devuelve el resultado si se muestra un mensaje de error.

Habilite o deshabilite la funcionalidad MFA de SnapCenter para la API de REST, la interfaz de línea de comandos y la interfaz gráfica de usuario

GUI

- Pasos*
  1. Inicie sesión en el servidor de SnapCenter como administrador de SnapCenter.
  2. Haga clic en **Ajustes** > **Ajustes globales** > **Ajustes de autenticación multifactorAuthentication(MFA)**
  3. Seleccione la interfaz (GUI/RST API/CLI) para habilitar o deshabilitar el inicio de sesión MFA.

Interfaz PowerShell

- Pasos*

  1. Ejecute los comandos de PowerShell o la CLI para habilitar la MFA en la interfaz gráfica de usuario, la API de REST, PowerShell y SCCLI.

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

     El parámetro PATH especifica la ubicación del archivo xml de metadatos de MFA de AD FS.

  Habilita la MFA para la interfaz gráfica de usuario de SnapCenter, la API de REST, PowerShell y SCCLI configuradas con la ruta de archivo de metadatos de AD FS especificada.

  1. Compruebe el estado y la configuración de MFA mediante `Get-SmMultiFactorAuthentication` cmdlet.

Interfaz SCCLI

- Pasos*

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

API REST

1. Ejecute la siguiente API posterior para habilitar la MFA en la interfaz gráfica de usuario, la API de REST, PowerShell y SCCLI.

Parámetro	Valor
Dirección URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Publicación

Cuerpo de la solicitud	{
	«IsGuiMFAEnabled»: Falso,
	«IsRestApiMFAEnabled»: Verdadero,
	«IsCliMFAEnabled»: Falso,
	ADFSConfigFilePath: C:\\ADFS_metadata\\abc.xml
	}

Cuerpo de respuesta	{
	«MFAConfiguration»: {
	«IsGuiMFAEnabled»: Falso,
	«ADFSConfigFilePath»:
	«C:\\ADFS_metadata\\abc.xml»,
	«SCConfigFilePath»: Null,
	«IsRestApiMFAEnabled»: Verdadero,
	«IsCliMFAEnabled»: Falso,
	«ADFSHostName»: «win-adfs-sc49.winscedom2.com»
	}
	}

2. Compruebe el estado y la configuración de MFA mediante la siguiente API.

Parámetro	Valor
Dirección URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Obtenga

Cuerpo de respuesta	{
	«MFAConfiguration»: {
	«IsGuiMFAEnabled»: Falso,
	«ADFSConfigFilePath»:
	«C:\\ADFS_metadata\\abc.xml»,
	«SCConfigFilePath»: Null,
	«IsRestApiMFAEnabled»: Verdadero,
	«IsCliMFAEnabled»: Falso,
	«ADFSHostName»: «win-adfs-sc49.winscedom2.com»
	}
	}

Instale el servidor SnapCenter

Instale el servidor de SnapCenter en el host de Windows

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. Debe utilizar PowerShell 7.4.2 o posterior.

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

Antes de empezar

- 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:\"`

Funciones habilitadas en el 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 Estos podrían ser de interés para solucionar problemas y realizar mantenimiento al

sistema host.

Categoría	Función
Servidor web	• Servicios de Información de Internet • Servicio World Wide Web • Características HTTP comunes ◦ Documento predeterminado ◦ Exploración de directorios ◦ Errores HTTP ◦ Redirección HTTP ◦ Contenido estático ◦ Publicación en WebDAV • Estado y diagnóstico ◦ Registro personalizado ◦ Registro HTTP ◦ Herramientas de registro ◦ Supervisor de solicitudes ◦ Seguimiento • Características de rendimiento ◦ Compresión de contenido estático • Seguridad ◦ Seguridad IP ◦ Autenticación básica ◦ Compatibilidad centralizada con certificados SSL ◦ Autenticación por asignación de certificados de clientes ◦ Autenticación de asignaciones de certificado de cliente de IIS ◦ Restricciones de IP y dominio ◦ Filtrado de solicitudes ◦ Autorización para URL ◦ Autenticación de Windows • Características de desarrollo de aplicaciones ◦ Extensibilidad de .NET 4.5 ◦ Inicialización de aplicaciones ◦ ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle ◦ Inclusión del lado servidor ◦ Protocolo WebSocket Herramientas de gestión Consola de gestión de IIS

Categoría	Función
Scripts y herramientas de gestión de IIS	• Servicio de gestión de IIS • Herramientas de gestión web
.NET Framework 8.0.12 Features	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • Activación HTTP de Windows Communication Foundation (WCF) 45 ◦ Activación de TCP ◦ Activación HTTP Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla para sistemas heredados que no tienen conectividad a Internet".
Servicio de activación de procesos de Windows	Modelo de proceso
API de configuración	Todo

Instale el servidor SnapCenter en el host Linux

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

Antes de empezar

- Si desea instalar SnapCenter Server con usuarios que no sean raíz y no tengan suficientes privilegios para instalar SnapCenter, obtenga el archivo de suma de comprobación sudoers del sitio de soporte de NetApp. Debe utilizar el archivo de suma de comprobación adecuado basado en la versión de Linux.
- Si el paquete sudo no está disponible en SUSE Linux, instale el paquete sudo para evitar errores de autenticación.
- Para SUSE Linux, configure el nombre de host para evitar el fallo de instalación.
- Compruebe el estado seguro de Linux ejecutando el comando `sestatus`. Si el estado *SELinux* está activado y el modo *CURRENT* es forzado, realice lo siguiente:
  - Ejecute el comando: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    El valor predeterminado de *WEBAPP_EXTERNAL_PORT* es 8146
  - Si el firewall bloquea el puerto, ejecute `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    El valor predeterminado de *WEBAPP_EXTERNAL_PORT* es 8146
  - Ejecute los siguientes comandos desde el directorio en el que tiene permiso de lectura y escritura:
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

Si el comando devuelve nada que hacer, vuelva a ejecutar el comando después de instalar SnapCenter Server.

- Si el comando crea *my-nginx.pp*, ejecute el comando para activar el paquete de políticas: `sudo semodule -i my-nginx.pp`

◦ La ruta de acceso utilizada para el directorio PID de MySQL es */var/opt/mysqld*. Ejecute los siguientes comandos para establecer los permisos para la instalación de MySQL.

- `mkdir /var/opt/mysqld`
- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
- `sudo restorecon -Rv /var/opt/mysqld`

◦ La ruta utilizada para el directorio Data de MySQL es */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Ejecute los siguientes comandos para establecer los permisos para el directorio de datos de MySQL.

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

Acerca de esta tarea

- Cuando el servidor SnapCenter está instalado en el host Linux, se instalan servicios de terceros como MySQL, RabbitMQ, Errlang. No debe desinstalarlos.
- El servidor SnapCenter instalado en el host Linux no admite:
  - Alta disponibilidad
  - Plugins de Windows
  - Active Directory (admite solo los usuarios locales, tanto el usuario raíz como el no raíz con creds)
  - Autenticación basada en claves para iniciar sesión en SnapCenter
- Durante la instalación de . Tiempo de ejecución DE RED, si la instalación no resuelve las dependencias de *libicu* library, instale *libicu* ejecutando el comando: `yum install -y libicu`
- Si la instalación del servidor SnapCenter falla debido a la no disponibilidad de *PERL*, instale *PERL* ejecutando el comando: `yum install -y perl`

Pasos

1. Descargue lo siguiente desde "Sitio de soporte de NetApp" To */home directory*.
   - Paquete de instalación del servidor SnapCenter: **Snapcenter-linux-server-(el8/el9/sles15).bin**
   - Archivo de claves públicas: **Snapcenter_public_key.pub**
   - Respectivo archivo de firma - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. Valide el archivo de firma.
   `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Para la instalación que no sea root, agregue el contenido visudo especificado en **snapcenter_server_checksum_(el8/el9/sles15).txt** disponible junto con el instalador .bin.

4. Asigne el permiso de ejecución para el instalador .bin.
   `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Realice una de las acciones para instalar el servidor SnapCenter.

Si desea ejecutar…	Realice lo siguiente…
Instalación interactiva	`./snapcenter-linux-server-(el8/el9/sles15).bin` Se le pedirá que introduzca la siguiente información: • Puerto externo de la aplicación web que se utiliza para acceder al servidor SnapCenter fuera del host Linux. El valor predeterminado es 8146. • El usuario del servidor SnapCenter que instalará el servidor SnapCenter. • El directorio de instalación donde se instalarán los paquetes.

Si desea ejecutar…	Realice lo siguiente…
Instalación no interactiva	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` Ejemplo: Sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log Los registros se almacenarán en */var/opt/snapcenter/logs*. Parámetros que se deben transferir para instalar el servidor SnapCenter: • DWEBAPP_EXTERNAL_PORT: Puerto externo de la aplicación web que se utiliza para acceder al servidor de SnapCenter fuera del host de Linux. El valor predeterminado es 8146. • DWEBAPP_INTERNAL_PORT: Puerto interno de la aplicación web que se utiliza para acceder al servidor SnapCenter dentro del host Linux. El valor predeterminado es 8147. • DSMCORE_PORT: Puerto SMCore en el que se ejecutan los servicios smcore. El valor predeterminado es 8145. • DSCHEDULER_PORT: Puerto del programador en el que se ejecutan los servicios del programador. El valor predeterminado es 8154. • DSNAPCENTER_SERVER_USER: Usuario del servidor SnapCenter que instalará el servidor SnapCenter. Para *DSNAPCENTER_SERVER_USER*, el valor por defecto es el usuario que ejecuta Installer. • Duser_INSTALL_DIR: Directorio de instalación donde se instalarán los paquetes. Para *DUSER_INSTALL_DIR*, el directorio de instalación predeterminado es */OPT*. • DINSTALL_LOG_NAME: Nombre del archivo de registro donde se almacenarán los registros de instalación. Este es un parámetro opcional y, si se especifica, no se mostrarán registros en la consola. Si no especifica este parámetro, los registros se mostrarán en la consola y también se almacenarán en el archivo de registro predeterminado.

El futuro

- Si el estado *SELinux* está activado y el modo *CURRENT* es “forzado”, el servicio **nginx** no se inicia. Debe ejecutar los siguientes comandos:
  a. Vaya al directorio principal.
  b. Ejecute el comando: `journalctl -x|grep nginx`.
  c. Si el puerto interno de WebApp (8147) no puede escuchar, ejecute los siguientes comandos:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Ejecutar `setsebool -P httpd_can_network_connect on`

- DSELINUX: Si el estado *SELinux* está “activado”, el modo *CURRENT* es “forzado”, y ha ejecutado los comandos mencionados en la sección Antes de comenzar, debe especificar este parámetro y asignar el valor como 1. El valor predeterminado es 0.
- DUPGRADE: El valor predeterminado es 0. Especifique este parámetro y su valor como cualquier entero que no sea 0 para actualizar el servidor SnapCenter.

Funciones habilitadas en el host Linux durante la instalación

El servidor SnapCenter instala los siguientes paquetes de software que pueden ayudar a solucionar problemas y realizar el mantenimiento del sistema host.

- RabbitMQ
- Erlang

Registre SnapCenter

Si es nuevo en productos de NetApp y no tiene una cuenta de NetApp existente, debe registrar SnapCenter para habilitar el servicio de soporte.

Pasos

1. Después de instalar SnapCenter, vaya a **Ayuda > Acerca de**.
2. En el cuadro de diálogo *About SnapCenter*, anote la instancia de SnapCenter, un número de 20 dígitos que comienza por 971.
3. Haga clic en https://register.netapp.com.
4. Haga clic en **no soy un cliente registrado de NetApp**.
5. Especifique sus datos para registrarse.
6. Deje en blanco el campo Número de serie de referencia de NetApp.
7. Seleccione **SnapCenter** en la lista desplegable Línea de productos.
8. Seleccione el proveedor de facturación.
9. Introduzca el identificador de instancia de SnapCenter de 20 dígitos.
10. Haga clic en **Enviar**.

Inicie sesión en SnapCenter mediante la autorización de RBAC

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.

Antes de empezar

- 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.
- Si el servidor SnapCenter está instalado en el host Linux, debe iniciar sesión mediante la cuenta de usuario que se utilizó para instalar el servidor de SnapCenter.

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. El "Guía de referencia de cmdlets de SnapCenter Software" contiene 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 • Sufijo Username@UPN Por ejemplo, username@netapp.com • 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.

resultado

Aparecerá la página Dashboard.

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".

Si desea añadir el host de un plugin en SnapCenter que se ejecuta en el host de Linux, debe obtener el archivo de suma de comprobación de la ubicación: */opt/NetApp/snapcenter/SnapManagerWeb/Repository*.

A partir de la versión 6,0, se crea en el escritorio un acceso directo para SnapCenter PowerShell. Puede acceder directamente a los cmdlets de PowerShell de SnapCenter utilizando el acceso directo.

Inicie sesión en SnapCenter con la autenticación multifactor (MFA)

El servidor de SnapCenter admite MFA para la cuenta de dominio, que forma parte del directorio activo.

Antes de empezar

Debe tener la MFA habilitada. Para obtener más información sobre cómo habilitar MFA, consulte "Active la autenticación multifactor"

Acerca de esta tarea

- Solo se admite FQDN
- Los usuarios de grupos de trabajo y entre dominios no pueden iniciar sesión mediante MFA
- 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. En la página de inicio de sesión de AD FS, introduzca Username y Password.

   Cuando aparezca el mensaje de error nombre de usuario o contraseña no válida en la página AD FS, compruebe lo siguiente:

   - Si el nombre de usuario o la contraseña son válidos

     La cuenta de usuario debe existir en Active Directory (AD).

   - Si ha superado el número máximo de intentos permitidos que se estableció en AD
   - Si AD y AD FS están en funcionamiento

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 el servidor SnapCenter

Agregar y aprovisionar el sistema de almacenamiento

Añadir sistemas de almacenamiento

Deberías configurar el sistema de almacenamiento que le dé acceso a SnapCenter a almacenamiento de ONTAP, sistemas ASA R2 o Amazon FSx para NetApp ONTAP para realizar operaciones de protección de datos y aprovisionamiento.

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 FSX compuesta por varias SVM mediante la cuenta fsxadmin o añadir FSX SVM en SnapCenter.

Antes de empezar

- 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 snapshots 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. Los nombres de los sistemas de almacenamiento, sin incluir el nombre de dominio, deben tener 15 caracteres o menos, 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. 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. 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. Después de añadir la conexión de almacenamiento a SnapCenter, no debe cambiar el nombre de la SVM o el clúster mediante ONTAP. Si se añade SVM con un nombre corto o FQDN, debe poder resolverse tanto del SnapCenter como del host del plugin.

Para este campo…	Realice lo siguiente…
Nombre de usuario/Contraseña	Introduzca las credenciales del usuario de almacenamiento que tenga los privilegios necesarios para acceder al sistema de almacenamiento.
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. 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.

Si ha agregado SVM en SnapCenter, el usuario debe seleccionar el tipo de plataforma del menú desplegable manualmente.

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

   El puerto 443 predeterminado normalmente funciona.

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

   El valor predeterminado es 60 segundos.

d. 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.
e. Haga clic en **Guardar**.
   1. Haga clic en **Enviar**.

resultado

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
-to enable -noteto enable
```

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

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.

Aprovisionar almacenamiento en hosts Windows

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 solo admite discos básicos. No se admiten los discos dinámicos.
- Para GPT solo una partición de datos y para MBR se permite una partición primaria que tiene un volumen formateado con NTFS o CSVFS y tiene una ruta de montaje.
- Estilos de partición compatibles: GPT, MBR; en una máquina virtual UEFI de VMware, solo se admiten discos 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.

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 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.

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.

Si desea crear y formatear discos fuera de SnapCenter, sólo se admiten sistemas de archivos NTFS y CSVFS.

Antes de empezar

- 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. El tamaño del clúster varía según el sistema operativo y las aplicaciones.

En este campo…	Realice lo siguiente…
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. 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. 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. 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. 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.

Propiedad	Descripción
Utilice punto de montaje de volumen	Monte el disco en la ruta de unidad especificada en el campo adyacente. 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. 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. 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. Asegúrese de que el espacio disponible en el volumen sea suficiente para acomodar todo el almacenamiento de LUN que considere necesario.
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. Las particiones MBR pueden generar problemas de desalineación en los clústeres de conmutación al nodo de respaldo de Windows Server. 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. 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. 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. 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 snapshot antes de cambiar el tamaño de un LUN.
- Si se necesita restaurar un LUN de una snapshot realizada antes de cambiar el tamaño de la LUN, SnapCenter cambia automáticamente el tamaño del LUN al tamaño de la snapshot.

  Después de la operación de restauración, los daños añadidos al LUN después de su cambio de tamaño deben restaurarse desde una copia de Snapshot realizada antes 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.

Antes de empezar

- 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. 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.
Disco compartido	El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server. 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. 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. 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. 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. 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. 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. 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.

Antes de empezar

- 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. El nombre que se introduce para el recurso compartido también se utiliza como nombre del volumen. El nombre del recurso compartido: • Debe ser una cadena UTF-8. • No debe incluir los siguientes caracteres: Caracteres de control de 0x00 a 0x1F (ambos inclusive), 0x22 (comillas dobles) y los caracteres especiales `\ / [ ] : (vertical bar) < > + = ; , ?`
Comparta la ruta	• Haga clic en el campo para introducir una nueva ruta de acceso al sistema de archivos, por ejemplo, /. • 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.

Antes de empezar

- 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 GUI de SnapCenter para realizar trabajos de aprovisionamiento de host y recuperación de espacio, puede usar los cmdlets de PowerShell. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Si los cmdlets de PowerShell de SnapCenter se rompen debido a la eliminación de SnapDrive para Windows del servidor, consulte "Los cmdlets de SnapCenter se rompen cuando se desinstala SnapDrive para Windows".

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 snapshots.

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

  Admite controladoras SCSI paravirtual de VMware. Los discos RDM pueden admitir 256 discos.

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 utilizando el Plug-in for Windows. Debes crear y luego agregar la LUN compartida a cada máquina virtual en el clúster.

Información relacionada

Consulta "Documentación técnica de Broadcom" y busca documentación sobre la agrupación en clúster de máquinas virtuales entre hosts físicos y la creación de LUN compartidas FC RDM para clústeres de Microsoft.

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, AFF o ASA.

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

- Se agrega directamente al controlador de almacenamiento FAS, AFF o ASA mediante el Administrador del sistema ONTAP o la CLI de ONTAP .

> No ingresa ninguna información de licencia en la interfaz de usuario de SnapCenter para las licencias basadas en el controlador de SnapCenter .

- Se bloqueó en el número de serie de la controladora

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

Paso 1: Verifique si la licencia de SnapManager Suite está instalada

Puede utilizar la interfaz de usuario de SnapCenter para verificar si hay una licencia de SnapManager Suite instalada en los sistemas de almacenamiento primario FAS, AFF o ASA e identificar qué sistemas necesitan licencias. Las licencias de SnapManager Suite se aplican únicamente a SVM o clústeres FAS, AFF y ASA en sistemas de almacenamiento primario.

> Si ya tiene una licencia de SnapManager Suite en su controlador, SnapCenter proporciona automáticamente el derecho de licencia basado en controlador estándar. Los nombres licencia SnapManagerSuite y licencia basada en controlador SnapCenter Standard se usan indistintamente, pero hacen referencia a la misma licencia.

Pasos

1. En el panel de navegación izquierdo, selecciona **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 añadieron:
   - 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 selecciona el nombre del clúster, todas las SVM que son parte del clúster se muestran en la sección Storage Virtual Machines.
3. En la lista Storage Connections, localice la columna Controller License.

   La columna Controller License muestra el siguiente estado:

   - Indica que hay una licencia de SnapManager Suite instalada en un sistema de almacenamiento primario FAS, AFF o ASA.
   - Indica que no hay una licencia de SnapManager Suite instalada en un sistema de almacenamiento primario de FAS, AFF o ASA.
   - No aplicable indica que no es aplicable una licencia de la suite de SnapManager, ya que la controladora de almacenamiento está en Amazon FSx para plataformas de almacenamiento secundario, Cloud Volumes ONTAP, ONTAP Select o NetApp ONTAP.

Paso 2: Identificar 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, AFF o ASA.

El controlador muestra la licencia basada en el controlador SnapCenter Standard como la licencia SnapManagerSuite.

Pasos

1. Inicie sesión en la controladora de NetApp mediante la línea de comandos de ONTAP.
2. Ingrese el comando de visualización de licencia y luego vea el resultado para ver si la licencia de SnapManagerSuite está instalada.

   Resultado de ejemplo

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

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

Serial Number: 1-81-00000000000000000000000xx
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.

Paso 3: Recupere el número de serie de la controladora

Obtenga el número de serie del controlador mediante la línea de comando ONTAP . Debe ser un administrador de clúster en el sistema FAS, AFF o ASA para obtener su número de serie de licencia basado en controlador.

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.

Resultado de ejemplo

```
cluster1::> system show -instance

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

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

3. Registre los números de serie.

Paso 4: Recupere el número de serie de la licencia basada en controladora

Si utiliza almacenamiento FAS, ASA o AFF , puede recuperar la licencia basada en controlador de SnapCenter desde el sitio de soporte de NetApp antes de instalarlo usando la línea de comandos de ONTAP .

Antes de empezar

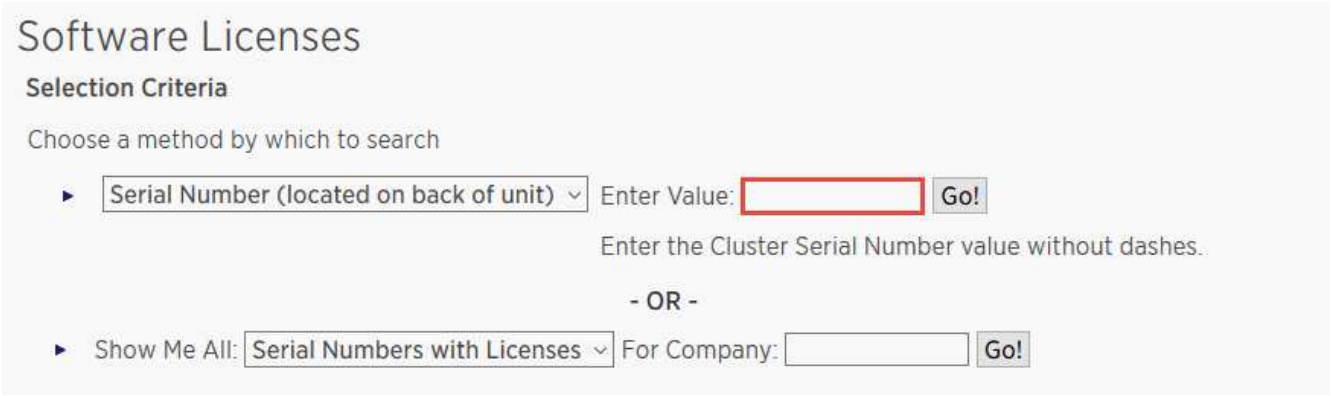
- Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.

Si no ingresa credenciales válidas, el sistema no devolverá ninguna información para su búsqueda.

- Debe tener el número de serie de la controladora.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp".
2. Vaya a **sistemas** > **licencias de software**.
3. En el área Criterios de selección, asegúrese de que está seleccionado Número de serie (ubicado en la parte posterior de la unidad), introduzca el número de serie del controlador y, a continuación, seleccione **Ir!**.



Se muestra una lista de licencias para la controladora especificada.

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

Paso 5: 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, AFF o ASA y tenga una licencia estándar o una licencia SnapManagerSuite de SnapCenter.

Antes de empezar

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

Acerca de esta tarea

Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS, AFF o ASA, 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.

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

```
license show
```

Paso 6: Eliminar la licencia de prueba

Si está utilizando una licencia estándar de SnapCenter basada en controlador y necesita eliminar la licencia de prueba basada en capacidad (número de serie que termina en “50”), debe usar los comandos MySQL para eliminar la licencia de prueba manualmente. La licencia de prueba no se puede eliminar mediante la interfaz 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.

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 establecer una conexión con el servidor SnapCenter para una cuenta SnapCenterAdmin.
   b. Ejecute el comando set-SmRepositoryPassword para restablecer la contraseña de MySQL.

      Para obtener información sobre los cmdlets, 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';
```

Configuración de la alta disponibilidad

Configurar servidores SnapCenter para alta disponibilidad

Para admitir la alta disponibilidad (HA) en SnapCenter que se ejecuta en Windows o en Linux, 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.

También es posible configurar balanceo de carga de red (NLB) para configurar la alta disponibilidad de SnapCenter. Debe configurar manualmente NLB fuera de la instalación de SnapCenter para tener alta disponibilidad.

Para un entorno de nube, puede configurar alta disponibilidad usando Elastic Load Balancing (ELB) de Amazon Web Services (AWS) y el balanceador de carga de Azure.

Configurar la alta disponibilidad con F5

Para obtener instrucciones sobre cómo configurar los servidores SnapCenter para alta disponibilidad mediante el balanceador de carga F5, 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 adicional

- 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 una configuración de balanceo de carga (NLB o F5), si se añade un host que está parcialmente resuelto por el host de NLB o F5 y si el host de SnapCenter no puede conectarse a este host, la página del host SnapCenter cambia entre los hosts inactivos y en ejecución con frecuencia. Para resolver este problema, debe asegurarse de que ambos hosts SnapCenter puedan resolver el host en un host de balanceo de carga de red o F5.
- Los comandos de SnapCenter para la configuración MFA deben ejecutarse en todos los hosts. La configuración de partes de confianza se debe realizar en el servidor de Active Directory Federation Services (AD FS) mediante los detalles del clúster F5. El acceso de interfaz de usuario de SnapCenter en el nivel de host se bloqueará una vez que se habilite la MFA.
- Durante la conmutación al nodo de respaldo, la configuración del registro de auditoría no se reflejará en el segundo host. Por lo tanto, debe repetir manualmente la configuración del registro de auditoría en el host pasivo F5 cuando vuelve a estar activo.

Configurar alta disponibilidad mediante el balanceo de carga de red (NLB)

Es posible configurar NLB para configurar SnapCenter High Availability. Debe configurar manualmente NLB fuera de la instalación de SnapCenter para tener alta disponibilidad.

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

Configuración de alta disponibilidad con AWS Elastic Load Balancing (ELB)

Puede configurar un entorno SnapCenter de alta disponibilidad en Amazon Web Services (AWS) configurando dos servidores SnapCenter en zonas de disponibilidad (AZ) independientes y configurándolos para conmutación automática al respaldo. La arquitectura incluye direcciones IP privadas virtuales, tablas de enrutamiento y sincronización entre bases de datos MySQL activas y en espera.

Pasos

1. Configure la IP de superposición privada virtual en AWS. Para obtener más información, consulte "Configurar IP de superposición privada virtual".
2. Prepare el host Windows
   a. La prioridad de la fuerza IPv4 es superior a IPv6:
      - Ubicación: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - Clave: DisabledComponents
      - Tipo: REG_DWORD
      - Valor: 0x20
   b. Asegúrese de que los nombres de dominio completo se puedan resolver mediante DNS o mediante una configuración de host local en las direcciones IPv4.
   c. Asegúrese de que no tiene configurado un proxy del sistema.
   d. Asegúrese de que la contraseña del administrador sea la misma en Windows Server cuando utilice una configuración sin Active Directory y los servidores no estén en un dominio.
   e. Agregue IP virtual en ambos servidores Windows.
3. Cree el clúster de SnapCenter.
   a. Inicie PowerShell y conéctese a SnapCenter.
      ```
      Open-SmConnection
      ```
   b. Cree el clúster.
      ```
      Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip>
      -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator
      ```
   c. Agregue el servidor secundario.
      ```
      Add-SmServer -ServerName <server_name> -ServerIP <server_ip>
      -CleanUpSecondaryServer -Verbose -Credential administrator
      ```
   d. Obtenga los detalles de alta disponibilidad.
      ```
      Get-SmServerConfig
      ```
4. Cree la función Lamda para ajustar la tabla de enrutamiento en caso de que el punto final IP privado virtual no esté disponible, supervisado por AWS CloudWatch. Para obtener más información, consulte "Cree una función Lambda".
5. Cree un monitor en CloudWatch para supervisar la disponibilidad del punto final de SnapCenter. Se configura una alarma para activar una función Lambda si no se puede acceder al punto final. La función Lambda ajusta la tabla de enrutamiento para redirigir el tráfico al servidor SnapCenter activo. Para obtener más información, consulte "Crear canarios sintéticos".
6. Implemente el flujo de trabajo utilizando una función STEP como alternativa a la supervisión de CloudWatch, proporcionando tiempos de conmutación por error más pequeños. El flujo de trabajo incluye una función de sonda Lambda para probar la URL de SnapCenter, una tabla DynamoDB para almacenar recuentos de fallos y la función Paso en sí.
   a. Utilice una función lambda para sondear la URL de SnapCenter. Para obtener más información, consulte "Crear función Lambda".
   b. Cree una tabla DynamoDB para almacenar el recuento de fallos entre dos iteraciones de funciones de pasos. Para obtener más información, consulte "Comience con la tabla DynamoDB".
   c. Cree la función Paso. Para obtener más información, consulte "Documentación de funciones de pasos".
   d. Pruebe un solo paso.

e. Pruebe la función completa.

f. Cree el rol de IAM y ajuste los permisos para poder ejecutar la función Lambda.

g. Cree un programa para activar la función Paso. Para obtener más información, consulte "Uso de Amazon EventBridge Scheduler para iniciar funciones de pasos".

Configure la alta disponibilidad con el balanceador de carga de Azure

Puede configurar un entorno de SnapCenter de alta disponibilidad con el balanceador de carga de Azure.

Pasos

1. Cree máquinas virtuales en un conjunto de escalas mediante el portal de Azure. El conjunto de escalas de máquinas virtuales de Azure le permite crear y administrar un grupo de máquinas virtuales equilibradas de carga. El número de instancias de máquina virtual puede aumentar o disminuir automáticamente en respuesta a la demanda o a un programa definido. Para obtener más información, consulte "Cree máquinas virtuales en un conjunto de escalas mediante el portal de Azure".
2. Después de configurar las máquinas virtuales, inicie sesión en cada máquina virtual en VM Set e instale SnapCenter Server en ambos nodos.
3. Cree el clúster en el host 1.
   ```
   Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
   ```
4. Agregue el servidor secundario.
   ```
   Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
   ```
5. Obtenga los detalles de alta disponibilidad.
   ```
   Get-SmServerConfig
   ```
6. Si es necesario, vuelva a generar el host secundario.
   ```
   Set-SmRepositoryConfig -RebuildSlave -Verbose
   ```
7. Conmutación al nodo de respaldo en el segundo host.
   ```
   Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
   ```

== Cambiar de NLB a F5 para 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*. Alternativamente, 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*. Alternativamente, 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".

Configurar el control de acceso basado en roles (RBAC)

Crear un rol

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

Para crear sus propios roles, es necesario iniciar sesión como el rol "SnapCenterAdmin".

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. Especifique un nombre y una descripción para el nuevo rol.

   Solo se pueden utilizar los siguientes caracteres especiales en los nombres de usuario y de grupo: espacio ( ), guion (-), guión bajo (_) y dos puntos (:).

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.

6. 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.
7. Haga clic en **Enviar**.

Añada un rol de RBAC de NetApp ONTAP mediante comandos de inicio de sesión de seguridad

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

Antes de empezar

- Identifique la tarea (o tareas) que desea realizar y los privilegios necesarios para realizar estas tareas.
- 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.
- Identifique su configuración dependiendo de si sus complementos de SnapCenter están conectados a la IP del administrador de clúster para todo el clúster o conectados directamente a una 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 para NetApp ONTAP, que se encuentra publicada 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 NetApp ONTAP agrega automáticamente la Privileges en el orden correcto, para que la Privileges de acceso total aparezca 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 NetApp 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".

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

"lun create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"volume qtree create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all

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

```
"nvme namespace show" -access all
```

Crear roles de SVM para sistemas ASA R2

Hay varios comandos CLI de ONTAP que debe ejecutar para crear una función para un nuevo usuario de SVM en sistemas ASA r2. Esta función es necesaria si configura SVM en sistemas ASA r2 para usar con SnapCenter y no desea utilizar la función 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
http -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 -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun igroup add" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume qtree modify" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all

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

"consistency-group" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all
- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

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 http -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 show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all

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

"system license show" -access all

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

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

"vserver cifs share modify" -access all

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

Cree roles de clúster de ONTAP para sistemas ASA R2

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 http -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 show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"lun igroup delete" -access all

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

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

"snapmirror policy show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume snapshot show-delta" -access all

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

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all`

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.

Antes de empezar

- 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.

  Sólo puede incluir los siguientes caracteres especiales en nombres de usuario y nombres de grupo: Espacio ( ), guión (-), subrayado (_) y dos puntos (:).

- 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 snapshots, 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 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. De forma predeterminada, se completa automáticamente con el nombre de dominio que ha iniciado sesión. Debe registrar el dominio que no es de confianza en la página **Configuración** > **Configuración global** > **Configuración de dominio**.
Tipo	Seleccione User o Group 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**. El nombre de usuario distingue entre mayúsculas y minúsculas. b. Seleccione el nombre de usuario en la lista de búsqueda. 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. 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.

Configure los ajustes del registro de auditoría

Se generan registros de auditoría para cada una de las actividades del servidor SnapCenter. De forma predeterminada, los registros de auditoría se protegen en la ubicación predeterminada instalada *C:\Program Files\NetApp\SnapCenter WebApp\audit*\.

Los registros de auditoría se protegen mediante la generación de resumen firmados digitalmente para cada uno de los eventos de auditoría para protegerlos de la modificación no autorizada. El resumen generado se mantiene en el archivo de suma de comprobación de auditoría independiente y se realizan comprobaciones de integridad periódicas para garantizar la integridad del contenido.

Inició sesión con el rol de administrador de SnapCenter.

Acerca de esta tarea

- Las alertas se envían en las siguientes situaciones:
  - La programación de comprobación de integridad del registro de auditoría o el servidor de syslog están habilitados o deshabilitados
  - Errores en la comprobación de integridad del registro de auditoría, el registro de auditoría o el registro del servidor de syslog
  - Poco espacio en disco
- El correo electrónico se envía sólo cuando la comprobación de integridad falla.
- Debe modificar simultáneamente las rutas del directorio de registro de auditoría y del directorio de registro de suma de comprobación de auditoría. Solo no puede modificar uno de ellos.
- Cuando se modifican las rutas del directorio de registro de auditoría y del directorio de registro de suma de comprobación de auditoría, no se puede realizar la comprobación de integridad en los registros de auditoría presentes en la ubicación anterior.
- Las rutas de acceso del directorio de registro de auditoría y del directorio de suma de comprobación de auditoría deben estar en la unidad local del servidor SnapCenter.

  No se admiten las unidades compartidas o montadas en red.

- Si el protocolo UDP se utiliza en la configuración del servidor de syslog, los errores debido a que el puerto está inactivo o no está disponible no se pueden capturar como un error o una alerta en SnapCenter.
- Puede utilizar los comandos Set-SmAuditSettings y Get-SmAuditSettings para configurar los registros de auditoría.

  La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se

puede obtener ejecutando Get-Help nombre_comando. Alternativamente, también puede consultar el "Guía de referencia de cmdlets de SnapCenter Software".

Pasos

1. En la página **Configuración**, vaya a **Configuración** > **Configuración global** > **Configuración del registro de auditoría**.
2. En la sección Registro de auditoría, introduzca los detalles.
3. Introduzca el directorio **Registro de auditoría** y el directorio **Registro de suma de comprobación de auditoría**
   a. Introduzca el tamaño máximo del archivo
   b. Introduzca el número máximo de archivos de registro
   c. Introduzca el porcentaje de uso de espacio en disco para enviar una alerta
4. (Opcional) Activar **Registrar hora UTC**.
5. (Opcional) Activar **Comprobación de integridad del registro de auditoría** y hacer clic en **Iniciar comprobación de integridad** para verificación de integridad bajo demanda.

   También puede ejecutar el comando **Start-SmAuditIntegrityCheck** para iniciar la comprobación de integridad bajo demanda.

6. (Opcional) habilite los registros de auditoría reenviados al servidor de syslog remoto e introduzca los detalles del servidor de syslog.

   Debe importar el certificado del servidor de syslog en la raíz de confianza para el protocolo TLS 1.2.

   a. Introduzca el host de servidor de syslog
   b. Introduzca el puerto del servidor de syslog
   c. Introduzca el protocolo de servidor de syslog
   d. Introduzca el formato RFC
7. Haga clic en **Guardar**.
8. Puede ver comprobaciones de integridad de auditoría y de espacio en disco haciendo clic en **Monitor** > **Jobs**.

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 SnapManager.web.ui.dll.config.

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

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

7. Actualice el archivo SnapManager.web.ui.dll.config con las rutas proporcionadas en la sección [client] del archivo my.inii.

   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 SnapManager.web.ui.dll.config en los dos nodos HA.

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

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

8. Actualice el archivo SnapManager.web.ui.dll.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.

Configure la autenticación basada en certificados

La autenticación basada en certificados mejora la seguridad al verificar la identidad del servidor de SnapCenter y los hosts de los plugins, lo que garantiza una comunicación segura y cifrada.

Habilite la autenticación basada en certificados

Para habilitar la autenticación basada en certificados para SnapCenter Server y los hosts del plugin de Windows, ejecute el siguiente cmdlet de PowerShell. Para los hosts del plugin de Linux, se habilita la autenticación basada en certificado cuando se habilita SSL bidireccional.

- Para habilitar la autenticación basada en certificados de cliente:

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

- Para desactivar la autenticación basada en certificados de cliente:

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

Exporte certificados de entidad de certificación (CA) del servidor SnapCenter

Es necesario exportar los certificados de CA del servidor de SnapCenter a los hosts del plugin mediante la consola de gestión de Microsoft (MMC).

Antes de empezar

Debe haber configurado el SSL bidireccional.

- 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 Certificados Snap-in, seleccione la opción **Cuenta de computadora** y luego haga clic en **Finalizar**.
4. Haga clic en **Console root** > **Certificados - Equipo local** > **Personal** > **Certificados**.
5. Haga clic con el botón derecho en el certificado de CA adquirido, que se utiliza para el servidor SnapCenter y, a continuación, seleccione **Todas las tareas** > **Exportar** para iniciar el asistente de exportación.
6. Realice las siguientes acciones en el asistente.

Para esta opción…	Haga lo siguiente…
Exportar clave privada	Seleccione **No, no exporte la clave privada** y luego haga clic en **Siguiente**.
Exportar formato de archivo	Haga clic en **Siguiente**.
Nombre de archivo	Haga clic en **Examinar** y especifique la ruta del archivo para guardar el certificado, y 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.

La autenticación basada en certificados no se admite para las configuraciones de alta disponibilidad de SnapCenter y el plugin de SnapCenter para VMware vSphere.

Importe el certificado de CA a los hosts del plugin de Windows

Para usar el certificado de CA de servidor de SnapCenter exportado, es necesario importar el certificado relacionado a los hosts del plugin de Windows de SnapCenter 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 Certificados Snap-in, seleccione la opción **Cuenta de computadora** y luego haga clic en **Finalizar**.
  4. Haga clic en **Console root** > **Certificados - Equipo local** > **Personal** > **Certificados**.
  5. Haga clic con el botón derecho en la carpeta “Personal” y seleccione **Todas las tareas** > **Importar** para iniciar el asistente de importación.
  6. Realice las siguientes acciones en el asistente.

Para esta opción…	Haga lo siguiente…
Ubicación de tienda	Haga clic en **Siguiente**.
Archivo para importar	Seleccione el certificado de servidor SnapCenter que termina con la extensión .cer.
Almacén de certificados	Haga clic en **Siguiente**.
Finalización del Asistente para exportación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación.

Importe el certificado de CA en los hosts del plugin UNIX

Debe importar el certificado de CA a los hosts del plugin de UNIX.

Acerca de esta tarea

- Puede gestionar la contraseña del almacén de claves del SPL y el alias de la pareja de claves firmada de CA en uso.
- La contraseña para el almacén de claves SPL y para toda la contraseña de alias asociada de la clave privada deben ser la misma.
- 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 `SPL_KEYSTORE_PASS`.
  2. Cambie la contraseña del almacén de claves:
     `$ keytool -storepasswd -keystore 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>" -keystore keystore.jks`
  4. Actualice lo mismo para la clave spl_KEYSTORE_PASS IN `spl.properties` archivo.
  5. Reinicie el servicio después de cambiar la contraseña.

Configure los certificados intermedios o de raíz para el almacén de confianza SPL

Debe configurar los certificados intermedios o raíz para el almacén de confianza de SPL. Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves de 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`
  4. Añada un certificado raíz o intermedio:
     `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
  5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza de SPL.

Configure la pareja de claves firmados de CA para el almacén de confianza SPL

Debe configurar el par de claves firmado de CA como el almacén de confianza del SPL.

- Pasos*
  1. Navegue a la carpeta que contiene el almacén de claves del 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`
4. Agregue el certificado de CA con clave pública y privada.
   `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -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 almacén de claves de SPL es el valor de la clave spl_KEYSTORE_PASS in `spl.properties` archivo.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. 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`
2. Configure el nombre de alias desde el almacén de claves ubicado en `spl.properties` archivo. Actualice este valor contra la clave SPL_CERTIFICATE_ALIAS.
3. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza SPL.

Exportar certificados SnapCenter

Es necesario exportar los certificados de SnapCenter en formato .pfx.

- 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**.
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.

Configurar certificado de CA para el host de Windows

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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$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**.

> El sitio del programador de SnapCenter (el puerto predeterminado es 8154, HTTPS) está configurado con un certificado autofirmado. Este puerto se comunica dentro del host del servidor SnapCenter y no es obligatorio configurarlo con un certificado de CA. Sin embargo, si el entorno exige que utilice un certificado de CA, repita los pasos 5 a 9 con el sitio del programador de SnapCenter.

> 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.

Antes de empezar

- 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*. Alternativamente, 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 CA se ha validado correctamente.
- * * Indica que el certificado CA no se pudo validar.
- * * indica que no se ha podido recuperar la información de conexión.

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

Configurar certificado de CA para el host Linux

Después de instalar SnapCenter Server en Linux, el instalador crea el certificado autofirmado. Si desea utilizar el certificado CA, debe configurar los certificados para el proxy inverso nginx, el registro de auditoría y SnapCenter.

Configure el certificado nginx

Pasos

1. Vaya a */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Abra **snapcenter.conf** usando vi o cualquier editor de texto.
3. Navegue a la sección del servidor en el archivo de configuración.
4. Modifique las rutas de acceso de *ssl_certificate* y *ssl_certificate_key* para apuntar al certificado de CA.
5. Guarde y cierre el archivo.
6. Volver a cargar nginx: `$nginx -s reload`

Configure el certificado de registro de auditoría

Pasos

1. Abra *INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.ui.dll.config* utilizando vi o cualquier editor de texto.

   El valor predeterminado de *INSTALL_DIR* es */OPT*.

2. Edite las claves **AUDILOG_CERTIFICATE_PATH** y **AUDILOG_CERTIFICATE_PASSWORD** para incluir la ruta y contraseña del certificado CA respectivamente.

   Solo se admite el formato *.pfx* para los certificados de registro de auditoría.

3. Guarde y cierre el archivo.
4. Reinicie el servicio **snapmanagerweb**: `$ systemctl restart snapmanagerweb`

Configurar el certificado de SnapCenter

Pasos

1. Abra los siguientes archivos de configuración utilizando vi o cualquier editor de texto.
   - *INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.ui.dll.config*
   - *INSTALL_DIR/NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
   - *INSTALL_DIR/NetApp/snapcenter/Scheduler/Scheduler.api.dll.config*

   El valor predeterminado de *INSTALL_DIR* es */OPT*.

2. Edite las claves **SERVICE_CERTIFICATE_PATH** y **SERVICE_CERTIFICATE_PASSWORD** para incluir la ruta del certificado de CA y la contraseña respectivamente.

   Solo se admite el formato *.pfx* para el certificado de SnapCenter .

3. Guarde y cierre los archivos.
4. Reinicie todos los servicios.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Configure y habilite la comunicación SSL bidireccional en el host Windows

Configure la comunicación SSL bidireccional en el host de Windows

Es necesario configurar la comunicación SSL bidireccional para asegurar la comunicación mutua entre SnapCenter Server en el host de Windows y los plugins.

Antes de empezar

- Generó el archivo CSR de certificado de CA con la longitud mínima admitida de clave de 3072.
- El certificado de CA debe admitir la autenticación de servidor y la autenticación de cliente.
- Debe tener un certificado de CA con detalles de clave privada y huella digital.
- Debe haber activado la configuración SSL unidireccional.

  Para obtener información detallada, consulte "Configurar sección de certificado de CA."

- Debe haber habilitado la comunicación SSL bidireccional en todos los hosts del plugin y el servidor de SnapCenter.

  El entorno con algunos hosts o servidor no habilitado para la comunicación SSL bidireccional no está soportado.

Pasos

1. Para enlazar el puerto, ejecute los siguientes pasos en el host de servidor SnapCenter para el puerto 8146 del servidor web IIS de SnapCenter (predeterminado) y otra vez para el puerto 8145 de SMCore (predeterminado) mediante comandos de PowerShell.

a. Quite la vinculación de puertos de certificado autofirmado de SnapCenter existente mediante el siguiente comando de PowerShell.

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

Por ejemplo:

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

> netsh http delete sslcert ipport=0.0.0.0:8146
```

b. Enlace el certificado de CA recién adquirido con el servidor SnapCenter y el puerto SMCore.

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

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

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
certhash=$cert appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

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

Por ejemplo:

```
> $cert = "abc123abc123abc123abc123"

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

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

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

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

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

2. Para acceder al permiso al certificado de CA, añada el usuario del servidor web IIS predeterminado «**IIS AppPool\SnapCenter**» de SnapCenter en la lista de permisos de certificados siguiendo los siguientes pasos para acceder al certificado de CA recién adquirido.
   a. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar SnapIn**.
   b. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
   c. En la ventana del complemento certificados, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
   d. Haga clic en **raíz de consola** > **certificados – Equipo local** > **personal** > **certificados**.

e. Seleccione el certificado SnapCenter.

f. Para iniciar el asistente para agregar usuarios\permisos, haga clic con el botón derecho en el certificado de CA y seleccione **Todas las tareas** > **Gestionar claves privadas**.

g. Haga clic en **Agregar**, en el Asistente de selección de usuarios y grupos cambie la ubicación a nombre de equipo local (en la parte superior de la jerarquía)

h. Añada el usuario IIS AppPool\SnapCenter y proporcione permisos de control completos.

3. Para el permiso IIS del certificado **CA**, agregue la nueva entrada de claves de registro DWORD en el servidor SnapCenter desde la siguiente ruta:

   En el editor del registro de Windows, vaya a la ruta mencionada a continuación,

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
   ders\SCHANNEL
   ```

4. Cree una nueva entrada de clave de registro DWORD en el contexto de la configuración del registro SCHANNEL.

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

Configure el plugin de Windows de SnapCenter para la comunicación SSL bidireccional

Es necesario configurar el plugin de Windows de SnapCenter para la comunicación SSL bidireccional mediante comandos de PowerShell.

Antes de empezar

Asegúrese de que la huella digital del certificado de CA esté disponible.

Pasos

1. Para enlazar el puerto, realice las siguientes acciones en el host del plugin de Windows para el puerto SMCore 8145 (predeterminado).

   a. Quite la vinculación de puertos de certificado autofirmado de SnapCenter existente mediante el siguiente comando de PowerShell.

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

      Por ejemplo:

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

   b. Enlace el certificado de CA recién adquirido con el puerto SMCore.

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

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

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

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

Por ejemplo:

```
> $cert = "abc123abc123abc123abc123"

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

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

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

Habilite la comunicación SSL bidireccional en el host Windows

Es posible habilitar la comunicación SSL bidireccional para proteger la comunicación mutua entre SnapCenter Server en el host de Windows y los plugins mediante comandos de PowerShell.

Antes de empezar

Ejecute los comandos para todos los plugins y el agente de SMCore primero y luego para el servidor.

- Pasos*

1. Para habilitar la comunicación SSL bidireccional, ejecute los siguientes comandos en el servidor de SnapCenter para los plugins, el servidor y para cada uno de los agentes para los que se necesita la comunicación SSL bidireccional.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

1. Realice la operación de reciclaje del pool de aplicaciones de SnapCenter de IIS con el siguiente comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
2. Para los plugins de Windows, reinicie el servicio SMCore ejecutando el siguiente comando de PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Desactive la comunicación SSL bidireccional

Puede deshabilitar la comunicación SSL bidireccional mediante comandos de PowerShell.

Acerca de esta tarea

- Ejecute los comandos para todos los plugins y el agente de SMCore primero y luego para el servidor.
- Cuando deshabilita la comunicación SSL bidireccional, el certificado de CA y su configuración no se eliminan.
- Para añadir un nuevo host a SnapCenter Server, es necesario deshabilitar el SSL bidireccional para todos los hosts del plugin.
- NLB y F5 no son compatibles.
- Pasos*

1. Para deshabilitar la comunicación SSL bidireccional, ejecute los siguientes comandos en servidor de SnapCenter para todos los hosts del plugin y el host de SnapCenter.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

1. Realice la operación de reciclaje del pool de aplicaciones de SnapCenter de IIS con el siguiente comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
2. Para los plugins de Windows, reinicie el servicio SMCore ejecutando el siguiente comando de PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Configure y habilite la comunicación SSL bidireccional en el host Linux

Configure la comunicación SSL bidireccional en el host Linux

Debe configurar la comunicación SSL bidireccional para proteger la comunicación mutua entre el servidor de SnapCenter en el host de Linux y los plugins.

Antes de empezar

- Debe haber configurado el certificado de CA para el host Linux.
- Debe haber habilitado la comunicación SSL bidireccional en todos los hosts del plugin y el servidor de SnapCenter.

Pasos

1. Copie **certificate.pem** a */etc/pki/ca-trust/source/anchors/*.
2. Añada los certificados en la lista de confianza del host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`

3. Compruebe si los certificados se han agregado a la lista de confianza.
   `trust list | grep "<CN of your certificate>"`
4. Actualice **ssl_certificate** y **ssl_certificate_key** en el archivo **nginx** de SnapCenter y reinicie.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Actualice el enlace de la GUI del servidor de SnapCenter.
6. Actualice los valores de las siguientes claves en **snapmanager.web.ui.dll.config** que están ubicadas en _ /<installation path>/NetApp/snapcenter/SnapManagerWeb_ y **SMCoreServiceHost.dll.config** que están ubicadas en */<installation path>/NetApp/snapcenter/SMCore*.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
   - <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>
7. Reinicie los siguientes servicios.
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. Compruebe que el certificado esté conectado al puerto web de SnapManager.
   `openssl s_client -connect localhost:8146 -brief`
9. Compruebe que el certificado está conectado al puerto smcore.
   `openssl s_client -connect localhost:8145 -brief`
10. Gestione la contraseña del almacén de claves y el alias de SPL.
    a. Recuperar la contraseña predeterminada del almacén de claves SPL asignada a la clave **spl_KEYSTORE_PASS** en el archivo de propiedades spl.
    b. Cambie la contraseña del almacén de claves.
       `keytool -storepasswd -keystore keystore.jks`
    c. Cambie la contraseña de todos los alias de las entradas de clave privada.
       `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. Actualice la misma contraseña para la clave **spl_KEYSTORE_PASS** en *spl.properties*.
    e. Reinicie el servicio.
11. En el host Linux del plugin, añada los certificados raíz e intermedios en el almacén de claves del plugin de SPL.
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
      i. Compruebe las entradas en keystore.jks.
         `keytool -list -v -keystore <path to keystore.jks>`
      ii. Cambie el nombre de cualquier alias si es necesario.
         `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`

12. Actualice el valor de **spl_CERTIFICATE_ALIAS** en el archivo *spl.properties* con el alias **certificate.pfx** almacenado en *keystore.jks* y reinicie el servicio spl: `systemctl restart spl`
13. Compruebe que el certificado está conectado al puerto smcore.
`openssl s_client -connect localhost:8145 -brief`

Active la comunicación SSL en el host Linux

Es posible habilitar la comunicación SSL bidireccional para proteger la comunicación mutua entre el servidor SnapCenter en un host de Linux y los plugins mediante comandos de PowerShell.

Paso

1. Realice lo siguiente para activar la comunicación SSL unidireccional.
   a. Inicie sesión en la GUI de SnapCenter.
   b. Haga clic en **Ajustes** > **Ajustes globales** y seleccione **Habilitar validación de certificados en el servidor SnapCenter**.
   c. Haga clic en **Hosts** > **Managed Hosts** y seleccione el host del plugin para el que desea habilitar SSL unidireccional.
   d. Haga clic en el icono y, a continuación, haga clic en **Habilitar validación de certificado**.
2. Active la comunicación SSL bidireccional desde el host Linux del servidor SnapCenter.
   - `Open-SmConnection`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
   - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

Configure Active Directory, LDAP y LDAPS

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.

Antes de empezar

Protocolo LDAP y LDAPS

- Puede registrar los dominios de directorio activo que no son de confianza mediante los protocolos LDAP o LDAPS.
- 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.

Protocolo LDAP

- El nombre de dominio completo (FQDN) debe poder resolverse de SnapCenter Server.

  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 de una controladora de dominio y esto debe poder resolverse desde el servidor SnapCenter.

Protocolo LDAPS

- Los certificados DE CA son necesarios para que LDAPS proporcione un cifrado completo durante la comunicación del directorio activo.

  "Configure el certificado de cliente de CA para LDAPS"

- Se debe tener acceso a los nombres de host del controlador de dominio (DCHostName) desde el servidor SnapCenter.

Acerca de esta tarea

- Puede utilizar la interfaz de usuario de SnapCenter, los cmdlets de PowerShell o la API DE REST 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 para registrar un nuevo dominio.
  5. En la página Registrar nuevo dominio, seleccione **LDAP** o **LDAPS**.
     a. Si selecciona **LDAP**, especifique la información necesaria para registrar el dominio que no es de confianza para LDAP:

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. 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".

     b. Si selecciona **LDAPS**, especifique la información necesaria para registrar el dominio que no es de confianza para LDAPS:

Para este campo…	Realice lo siguiente…
Nombre de dominio	Especifique el nombre NetBIOS para el dominio.
Dominio FQDN	Especifique el FQDN.
Nombres de controladores de dominio	Especifique uno o más nombres de controladores de dominio y haga clic en **resolver**.
Direcciones IP del controlador de dominio	Si los nombres de los controladores de dominio no se pueden resolver desde el servidor SnapCenter, debe rectificar las resoluciones DNS.

6. Haga clic en **Aceptar**.

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.

Configure el certificado de cliente de CA para LDAPS

Debe configurar el certificado de cliente de CA para LDAPS en el servidor SnapCenter cuando la LDAPS de Windows con los certificados de CA.

- 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…
En la segunda página del asistente	Haga clic en **examinar**, seleccione el *Root Certificate* y 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.

7. Repita los pasos 5 y 6 para los certificados intermedios.

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.

- 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 importar backups desde SnapManager para Microsoft SQL Server a SnapCenter.

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

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 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 NetApp instantánea no disruptiva**

  El plugin para SQL Server utiliza la tecnología de Snapshot de NetApp con el plugin de NetApp SnapCenter para Microsoft Windows. 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 snapshots 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 memoria no volátil rápida (NVMe) en Windows Server 2022
  - Flujos de trabajo de backup, restauración, clonado y verificación en distribución de VMDK creada en NVMe over TCP/IP.
  - Es compatible con la versión de firmware 1,3 de NVMe a partir de la actualización 2 de ESX 8,0 y requiere la versión 21 de hardware virtual.
  - No se admite Windows Server Failover Clustering (WSFC) para aplicaciones a través de VMDK en NVMe sobre TCP/IP.
- Es compatible con la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo del sitio; es posible que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.

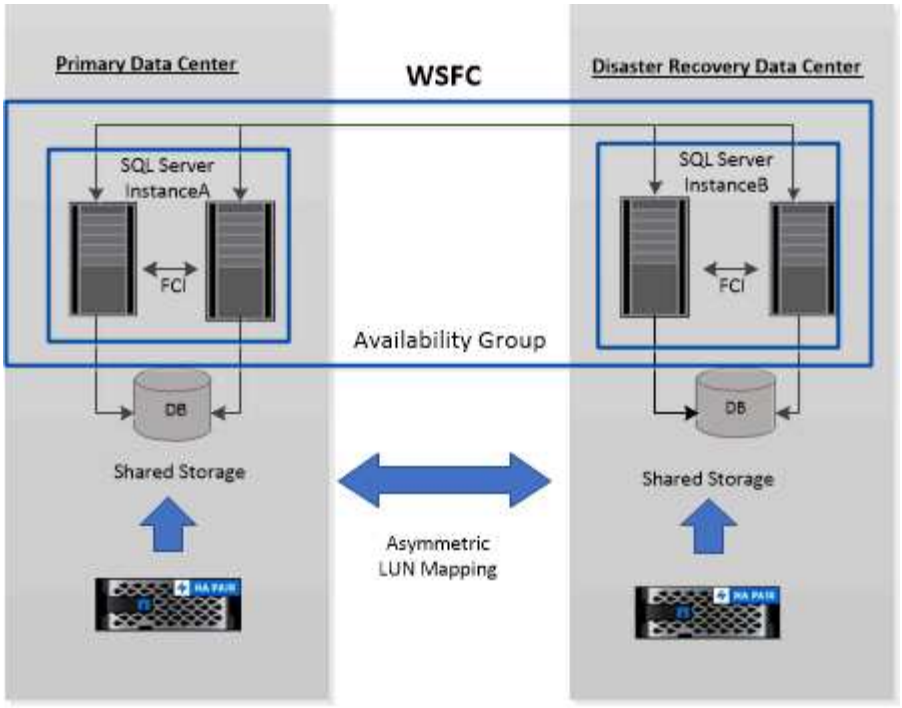
Compatibilidad con asignación de LUN asimétrica en clústeres de Windows

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 el plugin de SnapCenter para 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.

El soporte de aprovisionamiento y protección de datos de SnapCenter está disponible en Windows Server. Para obtener la información más reciente sobre las versiones compatibles, consulte la "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.
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.
Máquina virtual de VMware	Almacenes de datos VVOL en NFS y SAN	Herramientas de ONTAP para VMware vSphere	

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. 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. 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

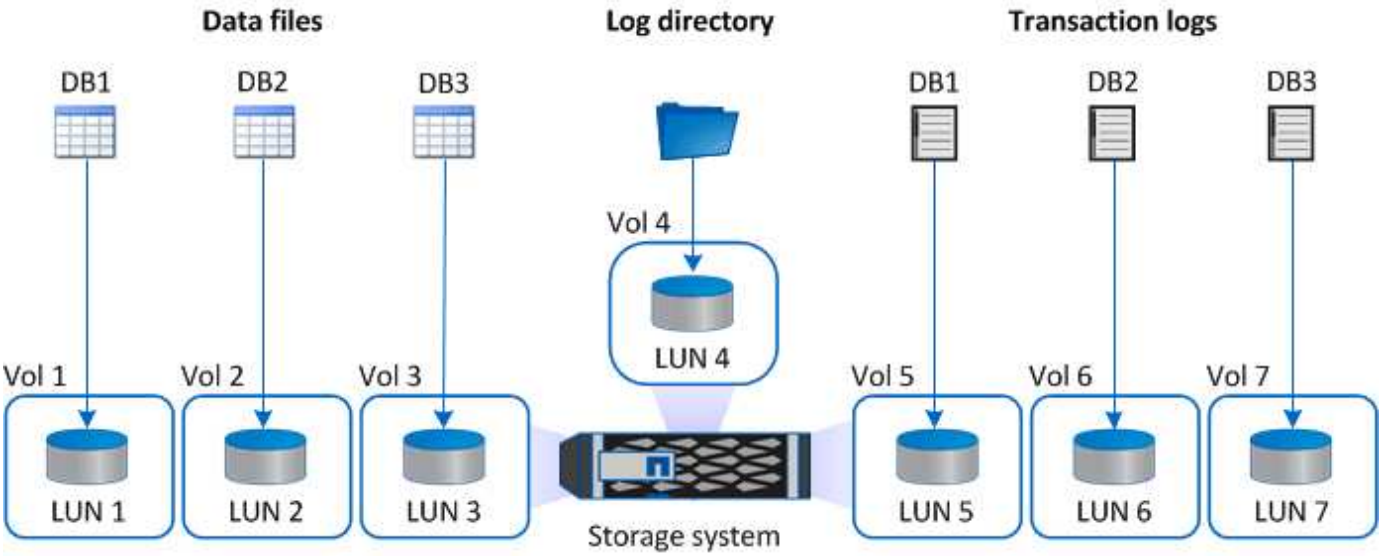
Para restaurar grandes bases de datos, la práctica recomendada es utilizar LUN o VMDK específicos El tiempo que se necesita para restaurar un LUN o un VMDK completos es inferior al que se requiere para

restaurar los archivos individuales almacenados en el LUN o el VMDK

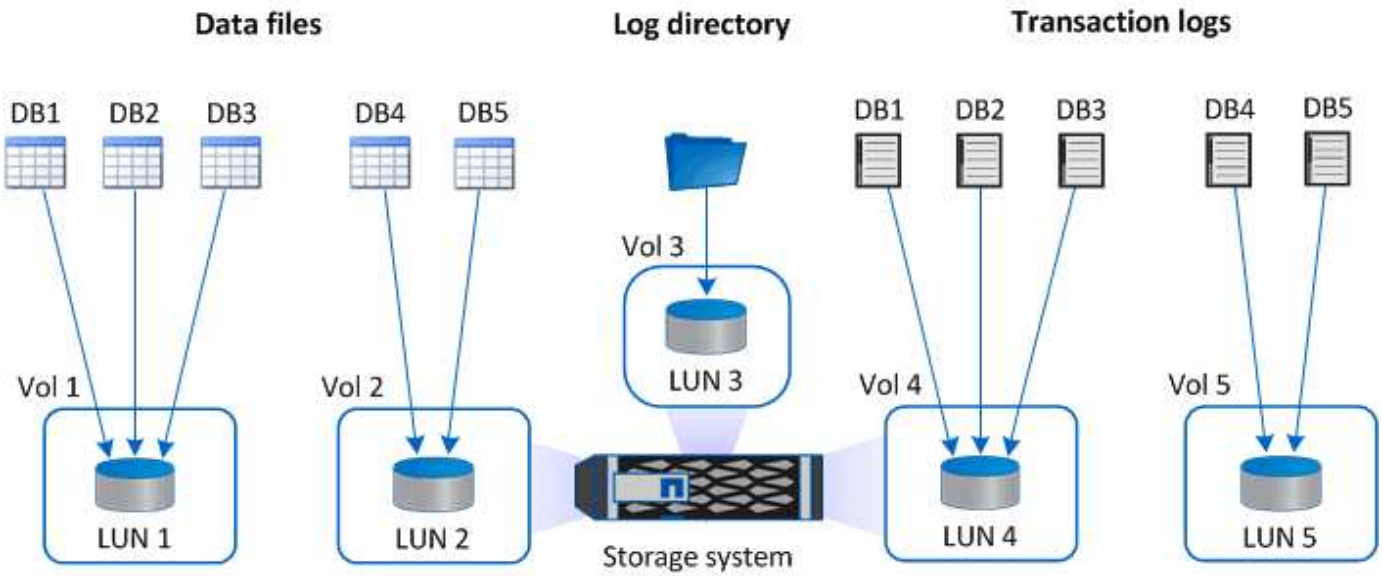
Para el directorio de registro, deber crear un LUN o un VMDK por separado para que haya espacio libre suficiente en los discos de archivos de registro o archivos de datos

Ejemplos de distribución de LUN y VMDK

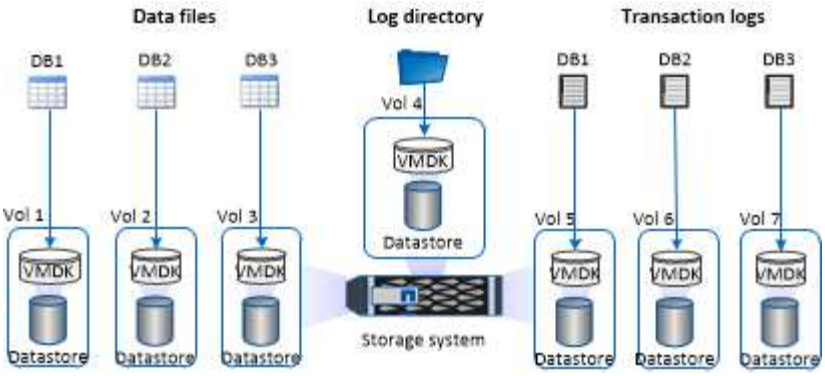
El gráfico siguiente muestra cómo puede configurar la distribución almacenamiento para bases de datos grandes en LUN:



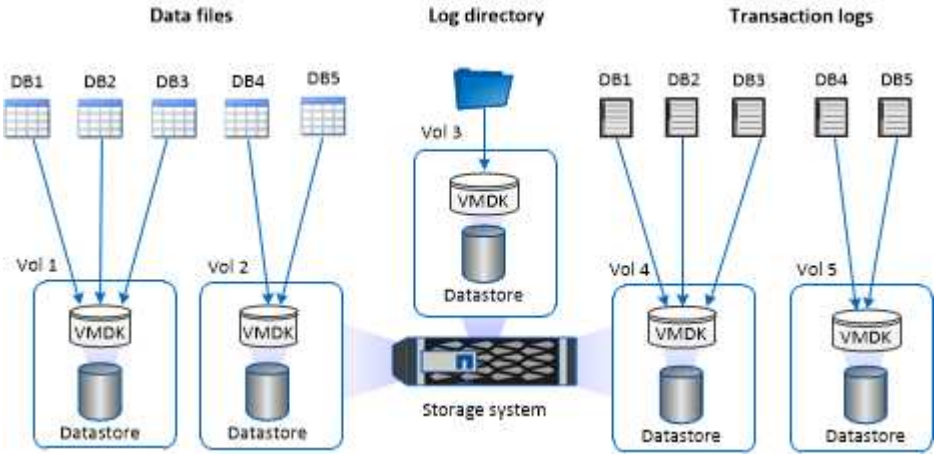
El gráfico siguiente muestra cómo puede configurar la distribución de almacenamiento para bases de datos medianas o pequeñas en LUN:



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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
- 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
- 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.

SnapCenter realiza las actualizaciones de SnapMirror y SnapVault después de completar la operación de

instantánea. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter . Si está utilizando la sincronización activa de SnapMirror , utilice las programaciones predeterminadas de SnapMirror o SnapVault tanto para la sincronización activa de SnapMirror como para las relaciones asincrónicas.

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 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. La instancia de SQL Server acorta los registros de transacciones eliminando las entradas que ya están confirmadas en la base de datos. 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. 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. 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. 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. 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. 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 Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la 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 Snapshot con 100 bases de datos en cada snapshot.

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 snapshots 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

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).

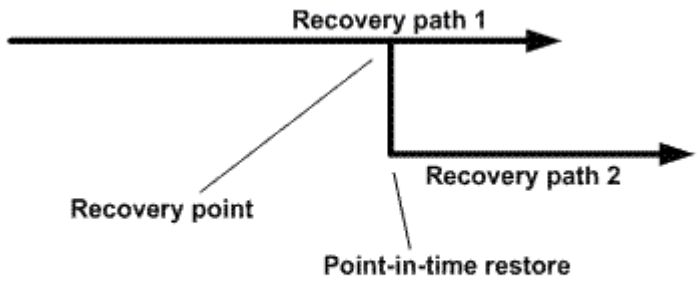
Restauración a un momento específico

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.

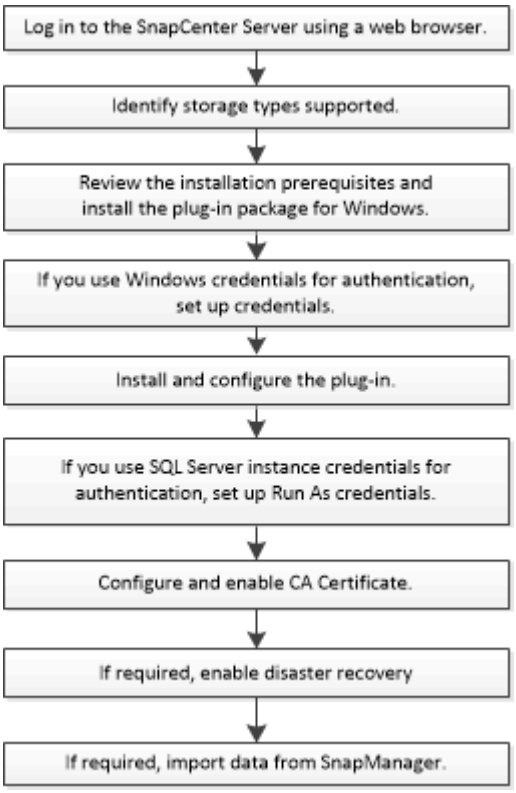
- Ciclo de vida de clon

Es posible utilizar SnapCenter para programar trabajos de clonado recurrentes que se producen cuando la base de datos de producción no está ocupada.

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>

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 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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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.

Antes de empezar

- 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 Settings, haga clic en **Credential**.
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. • Administrador del dominio 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: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • 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` 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, se recomienda asignar el mantenimiento de credenciales a un usuario o un grupo de usuarios en la página User and Access.

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 tanto del grupo de recursos como de backup.

Paso 1: Agregar y configurar credenciales

1. En el panel de navegación izquierdo, selecciona **Configuración**.
2. En la página Configuración, selecciona **Credencial**.
   a. Para agregar una nueva credencial, seleccione **Nuevo**.
   b. En la página Credential, configure las credenciales:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Introduzca un nombre para las credenciales.
Nombre de usuario	Introduzca el nombre de usuario utilizado para autenticación de SQL Server. • 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: ◦ *NetBIOS\Username* ◦ *Domain FQDN\Username* • 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*

Para este campo…	Realice lo siguiente…
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.

c. Seleccione **OK** para agregar la credencial.

Paso 2: Configurar instancias

1. En el panel de navegación izquierdo, selecciona **Recursos**.
2. En la página Resources, seleccione **Instance** en la lista **View**.
   a. Seleccione y, a continuación, seleccione el nombre del host para filtrar las instancias.
   b. Seleccione para cerrar el panel de filtros.
3. En la página Instance Protect, proteja la instancia y, si es necesario, seleccione **Configure Credentials**.

   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.
4. Seleccione **Actualizar recursos**.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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 2016 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 izquierdo, seleccione **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página hosts, haga lo siguiente:

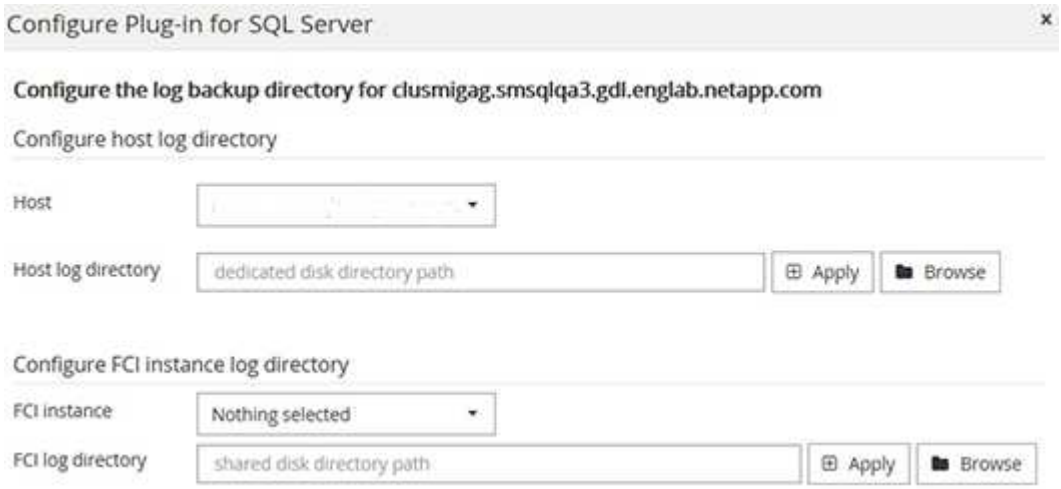
Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione Windows como tipo de host. El servidor de SnapCenter añade el host e instala el plugin para Windows si el plugin todavía no está instalado en el host. Si selecciona la opción de Microsoft SQL Server en la página Plug-ins, SnapCenter Server 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. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • WSFC 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. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. 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. Seleccione **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. 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.
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. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. 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. Seleccione **Enviar**.
8. Para el plugin de SQL, seleccione el host para configurar el directorio de registro.
   a. Seleccione **Configurar directorio de registro** y en la página Configurar directorio de registro de host, seleccione **Examinar** y complete los siguientes pasos:

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. Seleccione **Guardar**.

9. Seleccione **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.

10. 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.

Antes de empezar

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*. Alternativamente, 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.

4. 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.

Antes de empezar

- 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.

6. 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.
7. 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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$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.

Antes de empezar

- 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*. Alternativamente, 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 la recuperación ante desastres

Recuperación ante desastres del plugin de SnapCenter para SQL Server

Cuando el plugin de SnapCenter para SQL Server está inactivo, siga los siguientes pasos para cambiar a un host de SQL diferente y recuperar los datos.

Antes de empezar

- El host secundario debe tener el mismo sistema operativo, aplicación y nombre de host que el host primario.
- Inserte el complemento SnapCenter para SQL Server en un host alternativo utilizando la página **Agregar host** o **Modificar host**. Consulte "Gestionar hosts" si quiere más información.

Pasos

1. Seleccione el host en la página **hosts** para modificar e instalar el plugin de SnapCenter para SQL Server.
2. (Opcional) reemplace los archivos de configuración del plugin de SnapCenter para SQL Server desde un backup de recuperación ante desastres (DR) a la máquina nueva.
3. Importe las programaciones de Windows y SQL desde la carpeta del plugin de SnapCenter para SQL Server desde el backup de recuperación ante desastres.

Información relacionada

Vea "API de recuperación ante desastres" el vídeo.

Recuperación ante desastres de almacenamiento (DR) para el plugin de SnapCenter para SQL Server

Para recuperar el almacenamiento del plugin de SnapCenter para SQL Server, habilitar

el modo DR para almacenamiento en la página Global Settings.

Antes de empezar

- Compruebe que los plugins estén en modo de mantenimiento.
- Rompa la relación de SnapMirror/SnapVault."Romper las relaciones de SnapMirror"
- Conecte el LUN de secundario al equipo host con la misma letra de unidad.
- Asegúrese de que todos los discos estén conectados utilizando las mismas letras de unidad que se usaron antes de la recuperación ante desastres.
- Reinicie el servicio de servidor MSSQL.
- Asegúrese de que los recursos SQL vuelven a estar en línea.

Acerca de esta tarea

No se admite la recuperación ante desastres en las configuraciones VMDK y RDM.

Pasos

1. En la página Configuración, vaya a **Ajustes** > **Ajustes globales** > **recuperación ante desastres**.
2. Seleccione **Activar recuperación ante desastres**.
3. Haga clic en **aplicar**.
4. Compruebe si el trabajo DR está activado o no haciendo clic en **Monitor** > **trabajos**.

Después de terminar

- Si se crean bases de datos nuevas después de la conmutación al nodo de respaldo, las bases de datos se pondrán en modo sin recuperación ante desastres.

  Las nuevas bases de datos seguirán funcionando como lo hicieron antes del fallo.

- Los backups nuevos que se crearon en modo de recuperación ante desastres se enumeran en SnapMirror o SnapVault (secundario) en la página Topology.

  Se muestra un icono "i" junto a los nuevos backups para indicar que estos backups se han creado durante el modo de recuperación ante desastres.

- Puede eliminar los backups del plugin de SnapCenter para SQL Server que se crearon durante la conmutación por error usando la interfaz de usuario o el siguiente cmdlet de: `Remove-SmBackup`
- Después de la conmutación por error, si desea que algunos de los recursos estén en modo no DR, use el cmdlet siguiente: `Remove-SmResourceDRMode`

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

- SnapCenter Server gestionará los recursos de almacenamiento individuales (bases de datos SQL) que están en modo DR o no DR, pero no el grupo de recursos con recursos de almacenamiento que se encuentran en modo DR o en modo no DR.

Conmutación tras recuperación del plugin de SnapCenter para almacenamiento secundario de SQL Server al almacenamiento principal

Una vez que el almacenamiento primario del plugin de SnapCenter para SQL Server vuelve a estar en línea, debe recuperar el almacenamiento principal.

Antes de empezar

- Coloque el plugin de SnapCenter para SQL Server en el modo **Mantenimiento** de la página Managed hosts.
- Desconecte el almacenamiento secundario del host y conéctelo del almacenamiento primario.
- Para volver a realizar la conmutación tras recuperación al almacenamiento principal, asegúrese de que la dirección de la relación sigue siendo la misma que antes de la conmutación por error realizando la operación de resincronización inversa.

  Para conservar las funciones de almacenamiento primario y secundario después de la operación de resincronización inversa, realice de nuevo la operación de resincronización inversa.

  Para obtener más información, consulte "Volver a sincronizar las relaciones de reflejos"
- Reinicie el servicio de servidor MSSQL.
- Asegúrese de que los recursos SQL vuelven a estar en línea.

> Durante la conmutación por error o la conmutación tras recuperación del plugin, el estado general del plugin no se actualiza de forma inmediata. El estado general del host y el plugin se actualiza durante la operación de actualización del host posterior.

Pasos

1. En la página Configuración, vaya a **Ajustes** > **Ajustes globales** > **recuperación ante desastres**.
2. Deseleccione **Activar recuperación ante desastres**.
3. Haga clic en **aplicar**.
4. Compruebe si el trabajo DR está activado o no haciendo clic en **Monitor** > **trabajos**.

Después de terminar

Puede eliminar los backups del plugin de SnapCenter para SQL Server que se crearon durante la conmutación por error usando la interfaz de usuario o el siguiente cmdlet de: `Remove-SmDRFailoverBackups`

Instale el plugin de SnapCenter para VMware vSphere

Si su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM 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.
- 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.

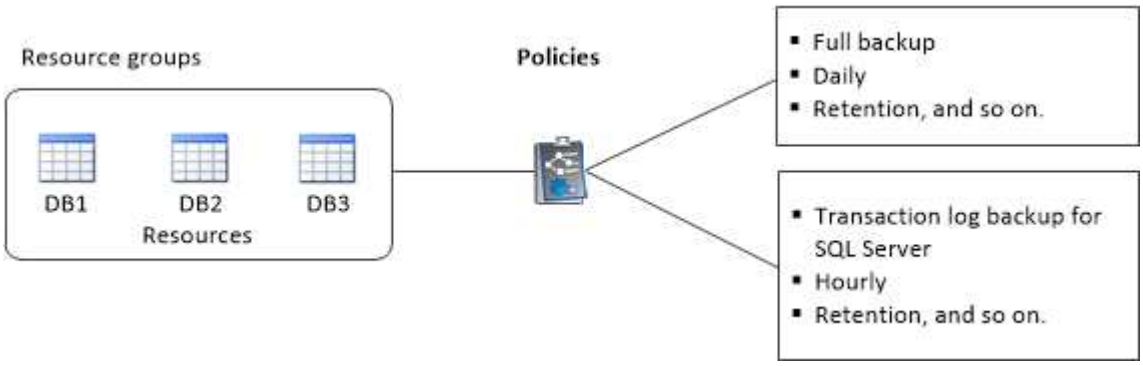
  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

- 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

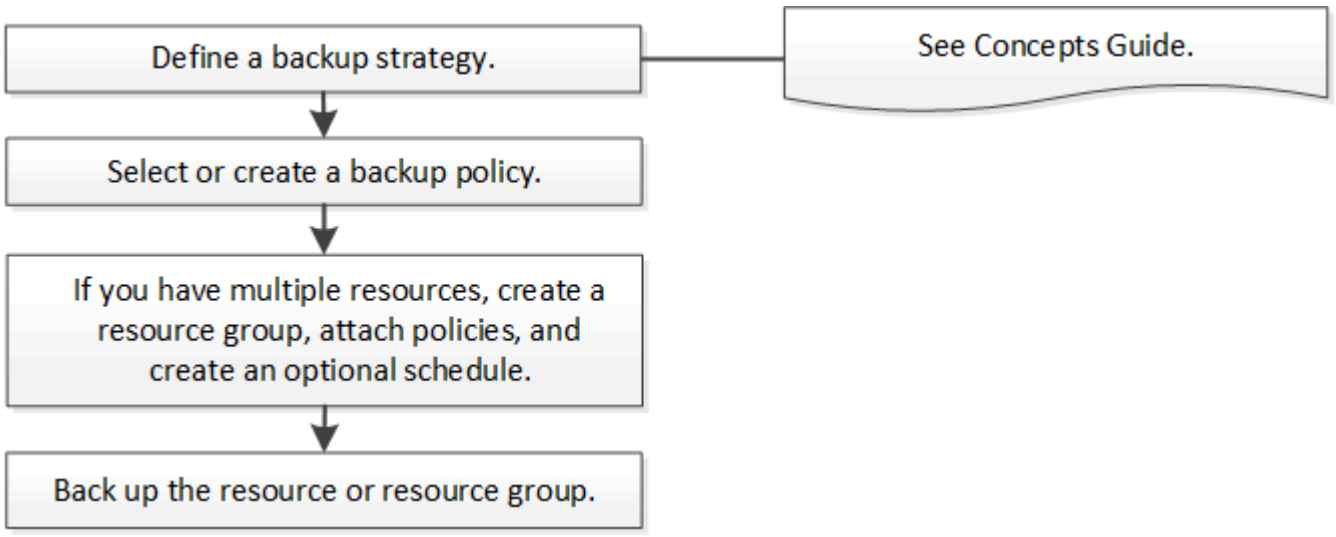
Flujo de trabajo de backup

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 la "Guía de referencia de cmdlets de SnapCenter Software"

Cómo SnapCenter hace backups de base de datos

SnapCenter utiliza la tecnología Snapshot para realizar backup de las bases de datos de SQL Server que residen en LUN o VMDK. Para crear el backup, SnapCenter crea 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.

Se realiza un backup simultáneo de todas las bases de datos que residen en un único volumen mediante Snapshot. 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 Snapshots 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 Snapshot en la política de backups.

Cuando SnapCenter crea una copia Snapshot, se captura todo el volumen del sistema de almacenamiento en la copia 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 Snapshot.

Más información

"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.

Antes de empezar

- 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 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 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 de 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.

   Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

   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.

1. 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.

Antes de empezar

- 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 Resources, seleccione **Database** o **Instance** en la lista desplegable **View**.
3. Seleccione la base de datos o la instancia de la lista y haga clic en **migrar**.
4. En la página Resources, 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**.
Elija Destinos	Seleccione la ubicación objetivo para los archivos de datos y de registro. 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. Esta opción no se muestra cuando selecciona el recurso **Instance**.

Para este campo…	Realice lo siguiente…
Opciones	Seleccione **Delete copy of Migrated Database at original Location** para eliminar la copia de la base de datos del origen. 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.
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. • Seleccione la opción **NO_INFOMSGS** para suprimir todos los mensajes informativos. • Seleccione la opción **ALL_ERRORMSGS** para visualizar todos los errores notificados por objeto. • Seleccione la opción **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. Se recomienda seleccionar esta opción para disminuir el tiempo de ejecución. • Seleccione la opción **TABLOCK** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una instantánea 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.

Antes de empezar

- 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 snapshots 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.

- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "Límites de objetos para la sincronización activa de SnapMirror".

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 RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.

    Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas

que el recuento especificado en la política.

Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

Paso 1: Crear nombre de política

1. En el panel de navegación izquierdo, selecciona **Configuración**.
2. En la página Configuración, selecciona **Políticas**.
3. Selecciona **Nuevo**.
4. En la página **Name**, introduzca el nombre y los detalles de la política.

Paso 2: Configure las opciones de política

1. En la página Policy type, realice los siguientes pasos:
   a. Seleccione el tipo de almacenamiento.
   b. Seleccione el ámbito de la política.

Backup completo y backup de registros

Realizar un backup de los archivos de la base de datos y los registros de transacciones y para truncar los registros de transacciones.

i. Seleccione **copia de seguridad completa y copia de seguridad de registro**.

ii. Introduzca el número máximo de bases de datos que se deben incluir en un backup para cada Snapshot.

> Debe aumentar dicho valor si desea ejecutar varias operaciones de backup en forma simultánea.

Backup completo

Realice un backup de los archivos de la base de datos.

i. Seleccione **copia de seguridad completa**.

ii. Introduzca el número máximo de bases de datos que se deben incluir en un backup para cada Snapshot.
El valor predeterminado es 100

> Debe aumentar dicho valor si desea ejecutar varias operaciones de backup en forma simultánea.

Backup de registros

i. Realice un backup de los registros de transacciones.

ii. Seleccione **copia de seguridad de registro**.

Copiar solo backup

i. 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.

Paso 3: Configure los ajustes del grupo de disponibilidad

1. En la sección Availability Group Settings, realice las siguientes acciones:

   a. Backup únicamente en la 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.

b. Seleccione replicas for backup.

   Seleccione la réplica principal o secundaria del AG para el backup.

c. Seleccionar prioridad de backup (prioridad de backup mínima y máxima)

   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.

   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.

Paso 4: Configure los ajustes de Snapshot y replicación

1. En la página Snapshot and Replication, realice los siguientes pasos:

   a. Especifique el tipo de programa seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

      Solo 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.

Paso 5: Configure los ajustes de retención actualizados al minuto

1. En la sección Up-to-the minute retention settings, según el tipo de backup seleccionado en la página de tipo de backup, realice una o más de las siguientes acciones:

Número específico de copias

Conserve únicamente una cantidad específica de snapshots.

1. 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.

Número específico de días

Retener las copias de backup por una cantidad determinada de días.

1. 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.

Paso 6: Configurar los ajustes de la instantánea

1. Para la configuración de retención de backup completo, realice las siguientes acciones:
   a. Especifique el número total de snapshots que desea conservar
      i. Para especificar el número de instantáneas a conservar, seleccione **Copias a conservar**.
      ii. Si la cantidad de copias de Snapshot supera el número especificado, las copias de Snapshot se eliminan empezando por las más antiguas.

> 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 snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva snapshot en el destino.

> El valor de retención máximo es 1018. Se producirá un error en los backups si la retención se establece con un valor superior al admitido por la versión de NetApp ONTAP subyacente.

2. El tiempo que se conservan las snapshots
   a. Si desea especificar el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas, seleccione **Retener copias para**.
3. Seleccione **Período de bloqueo de copia de instantánea** y especifique la duración en días, meses o años.

   El período de retención de SnapLock debe ser inferior a 100 años.

4. Seleccione una etiqueta de política.

> Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

Paso 7: Configure las opciones de replicación secundaria

1. En la sección Select secondary replication options, seleccione una de las siguientes opciones de

replicación secundaria o ambas:

Actualice SnapMirror

Actualice SnapMirror después de crear una copia snapshot local.

1. Seleccione esta opción para crear copias de SnapMirror de conjuntos de backups en otro volumen (SnapMirror).

   Esta opción debe estar habilitada para la sincronización activa de SnapMirror.

   Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.

   Consulte "Consulte los backups y los clones de SQL Server en la página Topology".

Actualizar SnapVault

Actualice SnapVault después de crear una copia snapshot.

1. Seleccione esta opción para realizar una replicación de backup de disco a disco.

   Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.

   Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP.

   Para obtener más información sobre el Almacén SnapLock, consulte "Confirmar copias Snapshot a WORM en un destino de almacén"

   Consulte "Consulte los backups y los clones de SQL Server en la página Topology".

Recuento de reintentos de error

1. Introduzca el número de intentos de replicación que deben producirse antes de que se interrumpa el proceso.

Paso 8: Configurar los ajustes de script

1. 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.

   Por ejemplo, se puede ejecutar un script para actualizar capturas SNMP, automatizar alertas y enviar registros.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

   Debe configurar la política de retención de SnapMirror en ONTAP para que el almacenamiento secundario no alcance el límite máximo de Snapshots.

Paso 9: Configure los ajustes de verificación

En la página Verification, realice los siguientes pasos:

1. En la sección Run verification for following backup schedules, seleccione la frecuencia de backup.
2. En la sección Database consistency check options, realice las siguientes acciones:
   a. Limitar la estructura de integridad a la estructura física de la base de datos (PHYSICAL_ONLY)
      i. 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.
   b. Suprimir todos los mensajes de información (NO INFOMSGS)
      i. Seleccione **Supress all information messages (NO INFOMSGS)** para suprimir todos los mensajes informativos. Seleccionado de forma predeterminada.
   c. Visualizar todos los mensajes de error notificados por objeto (ALL_ERRORMSGS)
      i. Seleccione **Display all reported error messages per object (ALL_ERRORMSGS)** para visualizar todos los errores notificados por objeto.
   d. No comprobar los índices no almacenados en clúster (NOINDEX)
      i. 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.
   e. Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una instantánea de la base de datos interna (TABLOCK)
      i. Seleccione **Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una copia Snapshot interna de la base de datos (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una instantánea interna de la base de datos.
3. 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.
4. 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.

> La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

Paso 10: Resumen de la revisión

1. Revisa el resumen y luego selecciona **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.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admite la adición de bases de datos nuevas sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de bases de datos nuevas a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

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**.

   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 los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba el nombre del grupo de recursos. 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: Introduzca un nombre y un formato de Snapshot personalizados. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

5. En la página Resources, 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 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. En la sección Configure schedules for selected policies, haga clic en * + en la columna Configure Schedules de la política para la cual 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 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 Set-SmSmtpServer de PowerShell.

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

Información relacionada

"Crear políticas de backup para bases de datos de SQL Server"

Cree grupos de recursos y habilite la protección secundaria para recursos de Microsoft SQL Server en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.

- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:

a. Seleccione el tipo de política de replicación.

No se admite la política de replicación síncrona.

b. Especifique el sufijo del grupo de consistencia que desea utilizar.

c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

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 desde 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.

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.

Antes de empezar

- 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 Core 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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 optimizar la operación de copia de seguridad, debe crear un registro de búsqueda inversa de nombres de clúster de Windows y direcciones IP en el servidor DNS.
- 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 gMSA tiene privilegios de inicio de sesión y administrador del sistema, gMSA puede conectarse a la instancia de SQL.
  - SnapCenter verificará si la autenticación para instancias SQL está configurada. Si la autenticación está configurada, se accederá a la instancia SQL con esta credencial.
  - Si la autenticación no está configurada, utilice gMSA para ver si el plugin de SQL está funcionando actualmente. Si el plugin funciona, se utilizará para establecer una conexión con la instancia de SQL.
  - Se accederá a la instancia de SQL mediante la autenticación de las credenciales de Windows cuando no se haya configurado la autenticación de las instancias de SQL y el plugin no esté operativo.

UI de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de 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 Resources, active la casilla de comprobación **custom name format for Snapshot copy** y, a continuación, introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

   Por ejemplo, customtext_policy_hostname o resource_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

4. En la página Policies, ejecute las siguientes tareas:

   a. En la sección Policies, seleccione una o más políticas de la lista desplegable.

      Puede crear una política seleccionando + para iniciar el asistente de políticas.

      En la sección **Configurar horarios para directivas seleccionadas**, se muestran las directivas seleccionadas.

   b. Seleccione + en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

   c. En la sección **Agregar horarios para la directiva** `policy_name` Cuadro de diálogo, configure la programación y, a continuación, seleccione * 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, a continuación, seleccione * * .

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. Seleccione **OK**.

Las programaciones configuradas figuran en la columna Applied Schedules.

6. 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 Set-SmSmtpServer de PowerShell.

7. Revisa el resumen y luego selecciona **Finalizar**.

Se muestra la página de topología de la base de datos.

8. Seleccione **Back up Now**.
9. 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. Seleccione **verificar después de la copia de seguridad** para verificar la copia de seguridad.

c. Seleccione **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. Para ver esto, seleccione el usuario o grupo correspondiente en la página acceso de usuario. El tipo de grupo de recursos implícito es "'recurso'".

10. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

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`.

Información relacionada

"Crear políticas de backup para bases de datos de SQL Server"

"Error de backup con programador de Windows"

"Error de operaciones de inactivación o agrupación de recursos"

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
```

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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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 izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos escribiendo su nombre en el cuadro de búsqueda o seleccionando y, luego, seleccionando la etiqueta. A continuación, puede seleccionar cerrar el panel de filtros.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **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. 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. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Información relacionada

"Crear políticas de backup para bases de datos de SQL Server"

"Crear grupos de recursos y asociar políticas para SQL Server"

"Error de backup con programador de Windows"

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

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 snapshots del almacenamiento si el backup creado no se registró en el servidor de SnapCenter. Si la copia de seguridad ya está registrada en el servidor de SnapCenter, no revertirá la copia snapshot ya creada incluso después de que se active la cancelación.

Antes de empezar

- 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.

Pasos

Ejecute una de las siguientes acciones:

Del…	Acción
Página Monitor	1. En el panel de navegación izquierdo, selecciona **Monitor** > **Trabajos**. 2. Seleccione el trabajo y seleccione **Cancelar trabajo** .
Panel de actividades	1. Después de iniciar la tarea de backup, seleccione En el panel Activity para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, seleccione **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, 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 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.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

- El sitio de réplica está activo.
- El sitio de réplica está inactivo.
- No se restableció la relación de reflejo o almacén secundario.

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 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 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 **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.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

   - Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse

manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.

- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.

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 almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

7. Seleccione un clon de la tabla y haga clic en **Clonar división**.
8. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .

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 Snapshot. Se recomienda utilizar este cmdlet cuando el total de las Snapshot que se muestran en la topología Manage Copies no corresponde al valor de retención de Snapshot del 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*. Alternativamente, 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.

   Este ejemplo borra el número de backups para backups secundarios sin snapshots:

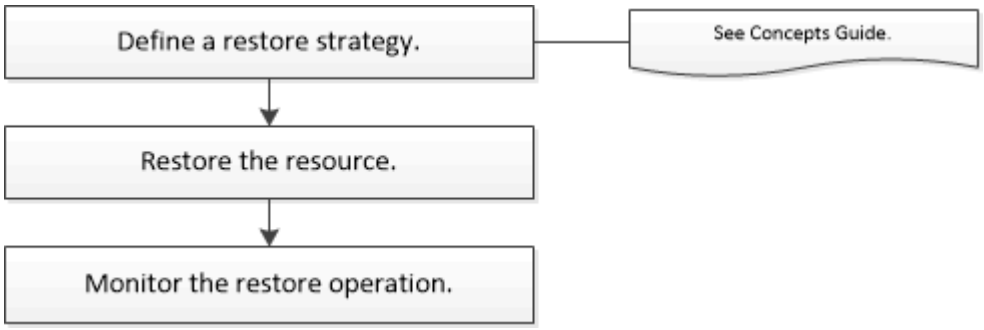
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

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 la "Guía de referencia de cmdlets de SnapCenter Software"

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 snapshots 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 puede configurarse es de 86400000 ms.

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 RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- La mayoría de los campos del asistente Restore son claros y explicativos. Aquí se ofrece información sobre los campos que podrían presentar dificultades.
- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.
- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

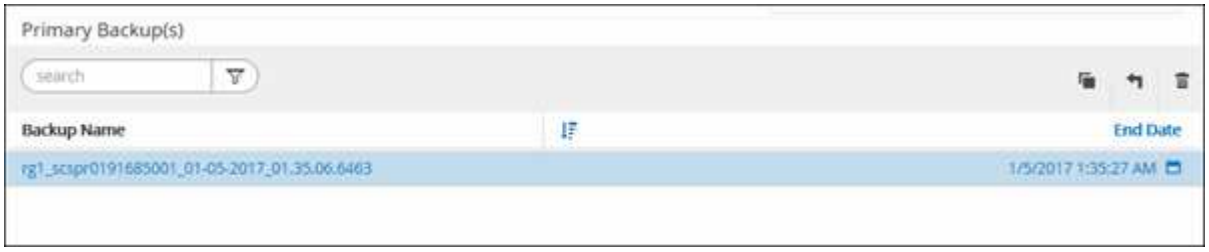
UI de SnapCenter

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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos o el grupo de recursos en la lista.

   Se muestra la página de topología.

4. En la vista Manage Copies, 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. Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración. La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original. 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. 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 Restore Scope, 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. 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. La opción **Usar directorio de registro personalizado** solo está disponible si ha seleccionado **Restaurar la base de datos a un host alternativo** o **Restaurar la base de datos utilizando archivos de base de datos existentes**. También puede utilizar la ruta de acceso compartida, pero asegúrese de que el usuario de SQL puede acceder a la ruta de acceso. 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 Pre Restore Options, 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.

      La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

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.

b. 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.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

10. 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.

11. Revise el resumen y, a continuación, haga clic en **Finalizar**.
12. Supervise el proceso de restauración mediante la página **Monitor** > **Jobs**.

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.

   ```
   PS C:\> Open-Smconnection
   ```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- Debe haber replicado las snapshots 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.

Acerca de esta tarea

Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 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**.

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.

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.

   ```
   PS C:\> Open-Smconnection
   ```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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 Resources, seleccione **Database** en la lista **View**.
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.

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

- Puede cancelar una operación de restauración en cola desde la página **Monitor** o desde el panel **actividad**.
- 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**. 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. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**.

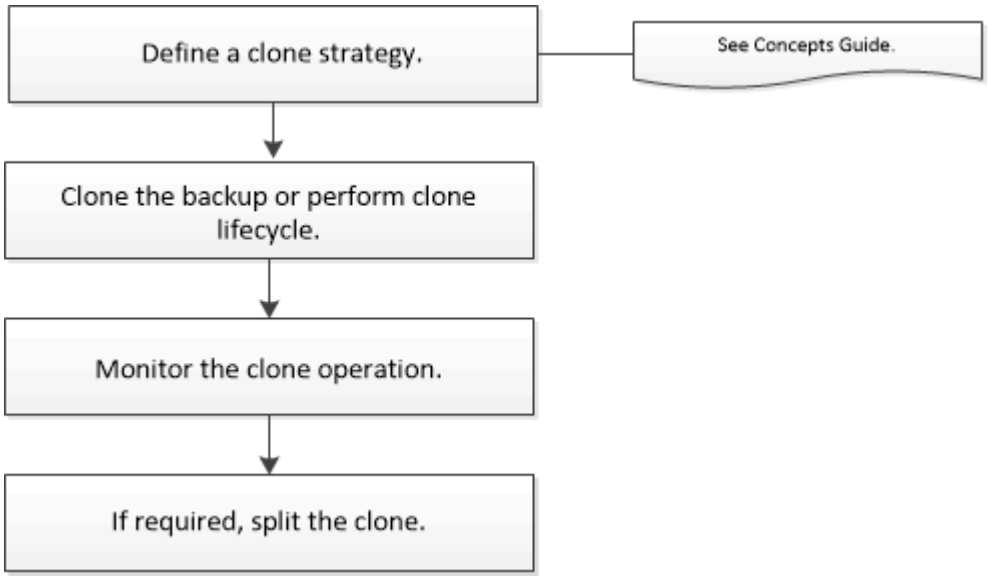
Clone recursos de bases de datos de SQL Server

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 cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración, recuperación, verificación y clonación. Para obtener información detallada sobre los cmdlets de PowerShell, utilice la ayuda de cmdlets de SnapCenter o consulte la documentación. "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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.
- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

  Para los entornos virtuales (VMDK/RDM), asegúrese de que el punto de montaje es un disco dedicado.

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione **SnapCenter Plug-in for SQL Server** de 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.

3. Seleccione la base de datos o el grupo de recursos.
4. En la página de visualización de **Manage Copies**, seleccione la copia de seguridad del sistema de almacenamiento principal o secundario (reflejado o en almacén).
5. Seleccione el backup y, a continuación, seleccione .
6. En la página **Clone Options**, 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. 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. 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.
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. 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.

7. 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. 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.

8. En la página **Script**, introduzca el tiempo de espera del script, la ruta y los argumentos del script previo o script 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.

   > La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

   El tiempo de espera predeterminado del script es 60 segundos.

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. 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"

10. Revisa el resumen y luego selecciona **Finalizar**.

11. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Después de crear el clon, no debe cambiar nunca el nombre.

Información relacionada

"Se produce un error en el clon de la base de datos de la instancia de clúster"

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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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.

Acerca de esta tarea

- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- La mayoría de los campos de las páginas del asistente Clone Lifecycle son autoexplicativos. Aquí se ofrece información sobre los campos que podrían presentar dificultades.
- Para ONTAP 9.12.1 y versiones posteriores, si especifica un período de bloqueo de instantánea, los clones creados a partir de las instantáneas a prueba de manipulación heredarán el tiempo de caducidad de la SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 el grupo de recursos o la base de datos y, a continuación, haga clic en **Clone Lifecycle**.
4. En la página Options, 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.

Para este campo…	Realice lo siguiente…
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 y los argumentos del script previo o script 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.

   > La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

   El tiempo de espera predeterminado del script es 60 segundos.

7. En la página Schedule, 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 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.

Para EMS, consulte "Gestione la recogida de datos de EMS"

9. 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

- Puede cancelar una operación de clonación en cola desde la página **Monitor** o desde el panel **actividad**.
- 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**. 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. 2. Seleccione la operación. 3. En la página **Detalles del trabajo**, haz 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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

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.

El complemento para bases de datos de SAP HANA es compatible con la sincronización activa de SnapMirror (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), que permite que los servicios empresariales sigan funcionando incluso si se produce un fallo completo del sitio. Esto permite que las aplicaciones realicen conmutaciones al nodo de respaldo de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.

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 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 Snapshot del grupo de consistencia (CG) 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 Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear snapshots 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
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • 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. 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. • LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creado • Volúmenes NFS conectados directamente con el Guest VM • Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos ONTAP requeridos para el plugin de SAP HANA

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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - lun

- lun create
- lun create
- lun create
- eliminación de lun
- igroup de lun añadido
- crear lun igroup
- lun igroup eliminado
- cambio de nombre de lun igroup
- 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
- modificación de snapshot de volumen: snaplock: tiempo de caducidad
- 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
- 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 8.3.0 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.

SnapCenter realiza las actualizaciones de SnapMirror y SnapVault después de completar la operación de instantánea. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter . Si está utilizando la sincronización activa de SnapMirror , utilice las programaciones predeterminadas de SnapMirror o SnapVault tanto para la sincronización activa de SnapMirror como para las relaciones asincrónicas.

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 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 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 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
- Varias instancias en el mismo host
- Escalado horizontal de varios niveles replicación de sistemas HANA
- Entorno de replicación en cascada en modo de replicación de sistemas

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 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 snapshots de grupos de consistencia

Es posible utilizar el plugin para crear snapshots 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 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 snapshots. 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 snapshot de grupos consistentes. La sincronización WAFL mejora el rendimiento de una 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.

Los snapshots 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 Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la 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, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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.

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, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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.

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.

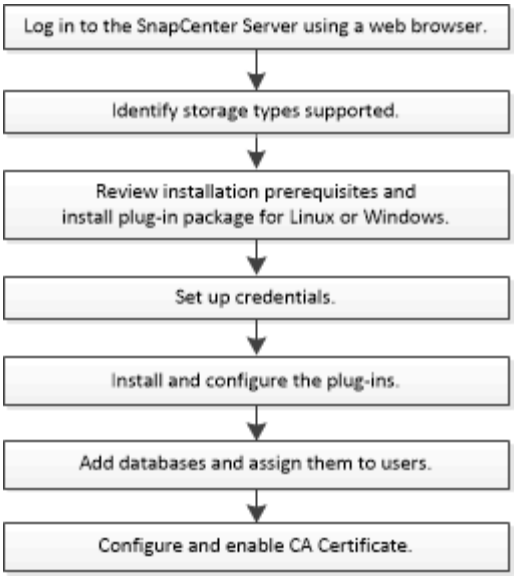
- Recuperar la base de datos hasta un backup de datos específico

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 11 en el host.

  IBM Java no es compatible con el host Windows y Linux.

- 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 11 en el host de Windows.

  "Descargar JAVA para todos los sistemas operativos"

Hosts Linux

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

  "Descargar JAVA para todos los sistemas operativos"

- 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.
- Debe tener **bash** como shell por defecto para la instalación del plug-in.

Comandos suplementarios

Para ejecutar un comando complementario en el plugin de SnapCenter para SAP HANA, debe incluirlo en el archivo *allowed_commands.config*.

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementarios en el host del plugin, abra el archivo *allowed_commands.config* en un editor. Escriba cada comando en una línea diferente y los comandos no distinguen mayúsculas de minúsculas. Asegúrese de especificar el nombre de ruta completamente cualificado y escribirlo entre comillas si contiene espacios.

Por ejemplo:

comando: mount

comando: umount

Comando: «C:\Program Files\NetApp\SnapCreator commands\sdcli.exe»

comando: myscript.bat

Si el archivo *allowed_commands.config* no está presente, los comandos o la ejecución del script se bloquearán y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

Si el comando o script no está presente en *allowed_commands.config*, el comando o la ejecución del script se bloqueará y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

No debe utilizar una entrada comodín (*) para permitir todos los comandos.

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. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- Para el usuario que no es root, asegúrese de que el nombre del usuario que no es root y del grupo del usuario debe ser el mismo.
- 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/*LINUX_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 HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux. .

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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 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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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 • SUSE Linux Enterprise Server (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Elemento	Requisitos
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 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	Java 11 Oracle Java y OpenJDK 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.

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

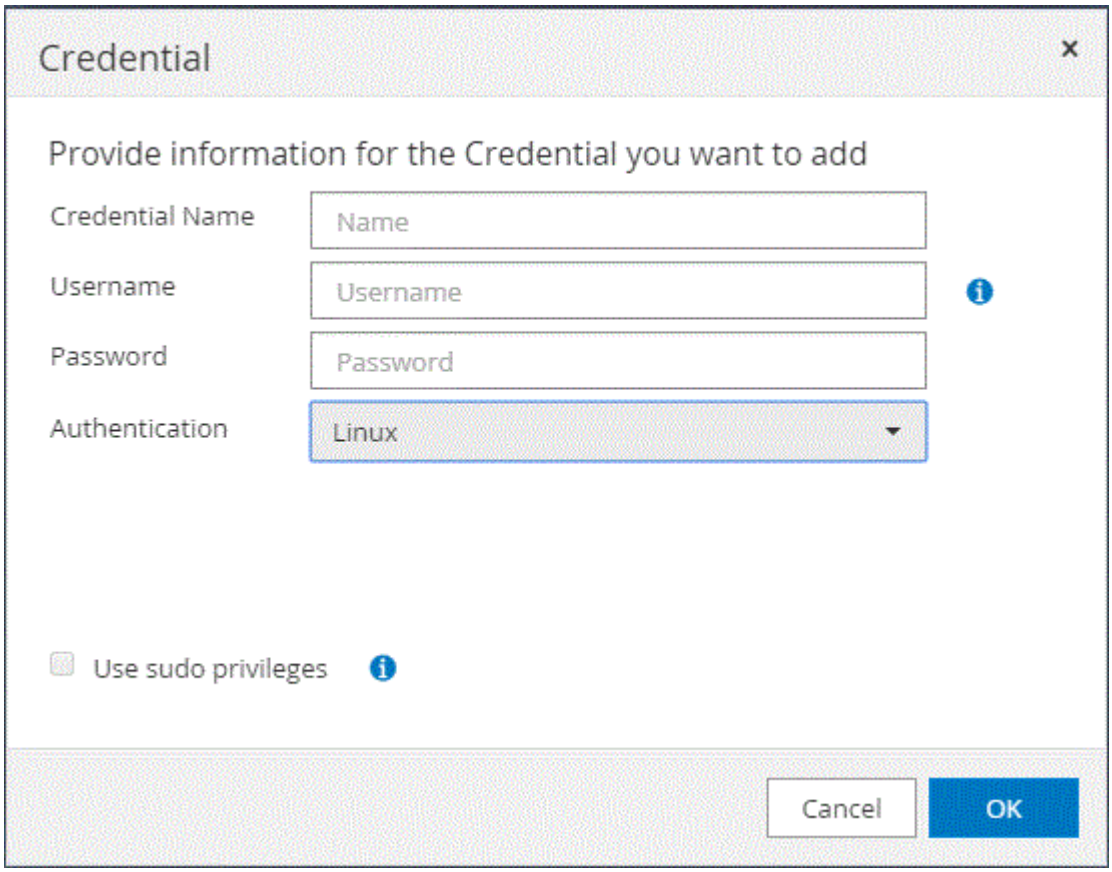
  Debe configurar credenciales de Windows antes de instalar plugins.

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 Settings, haga clic en **Credential**.
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. • 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* • 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* 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. Aplicable únicamente a usuarios Linux.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, se recomienda asignar el mantenimiento de credenciales

a un usuario o un grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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 2016 o posterior para SAP HANA"

Acerca de esta tarea

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Para la replicación de sistemas SAP HANA para descubrir recursos en sistemas primarios y secundarios, se recomienda añadir los sistemas primario y secundario que utilizan usuario raíz o sudo.

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: • Windows • Linux 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. 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. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado. 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. 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. • 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. • 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. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. 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.

9. 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.

Antes de empezar

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*. Alternativamente, 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.

4. 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).

Antes de empezar

- 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.

  El "Herramienta de matriz de interoperabilidad (IMT)" Contiene la información más reciente sobre las configuraciones compatibles.

- 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
```

4. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y añada el parámetro PLUGINS_ENABLED = hana:3.0.
5. 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*. Alternativamente, 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 solo se enumeren las operaciones de instalación de 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.

> La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Linux

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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 del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento: /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 para complementar el almacén de confianza.
   ```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento /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 del almacén de claves del complemento predeterminado es el valor de la clave 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 firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para complementos

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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 administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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*.

4. Reinicie el servicio después de cambiar la contraseña.

La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 para complementar el almacén de confianza.

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 del almacén de claves del complemento predeterminado es el valor de la clave

KEYSTORE_PASS en el archivo agent.properties.

Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos 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 de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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.

Antes de empezar

- 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*. Alternativamente, 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 su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM 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 11 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.

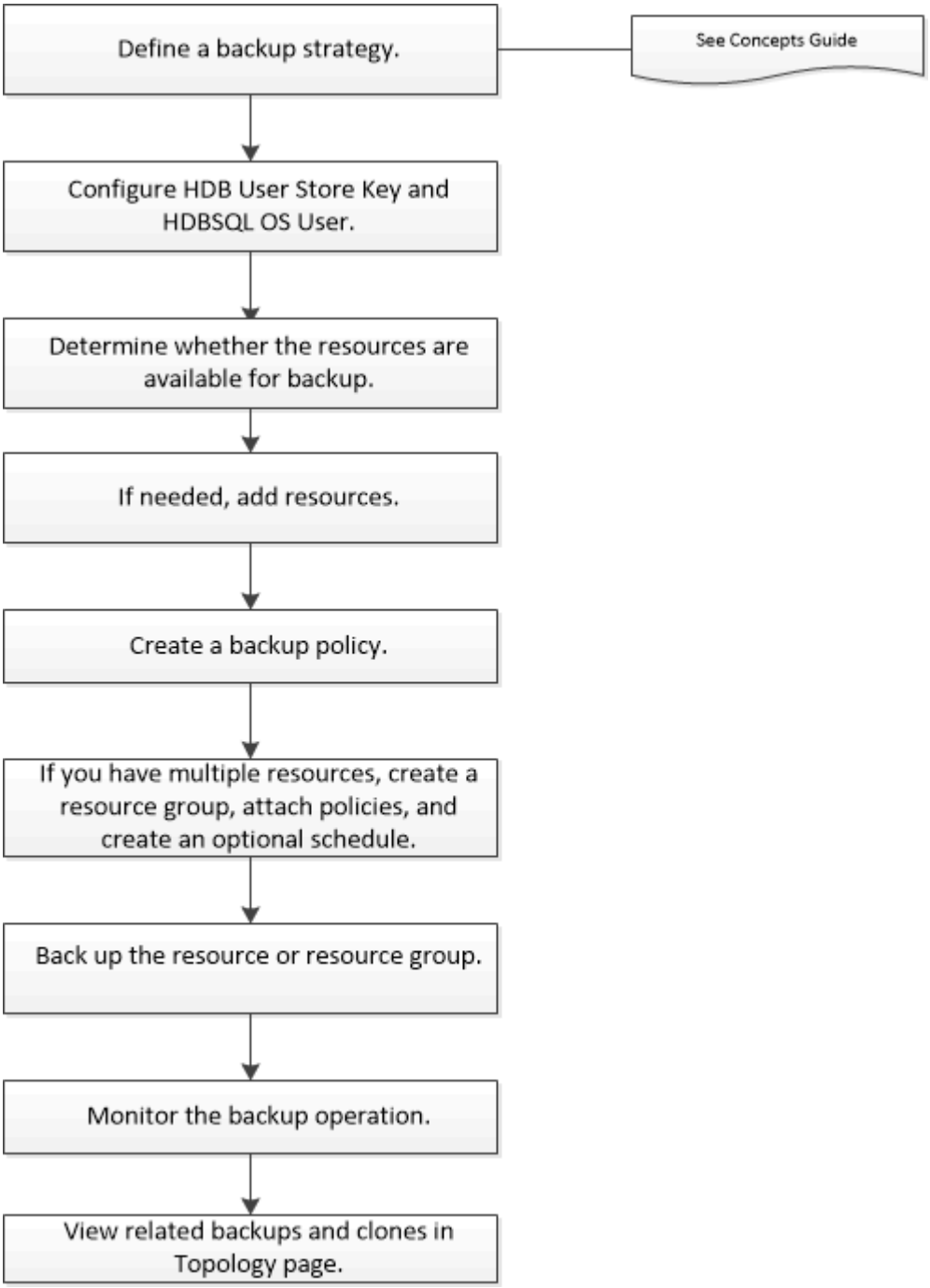
Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos 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. "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.

Antes de empezar

- 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 Resources, seleccione el tipo de recurso en la lista **View**.
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.

Antes de empezar

- 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 Resources, seleccione el tipo de recurso en la lista View.
3. (Opcional) Haga clic en y 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.

Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

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 Resources, 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 Snapshot primario es de 7 días y la retención de Snapshot secundarias es de 45 días, una vez completados 45 días y después de eliminar todos los backups, debe eliminar el grupo de recursos y el recurso de MDC anterior.

Información relacionada

"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.

Antes de empezar

- 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.
- Para la replicación del sistema SAP HANA, se recomienda añadir todos los recursos de ese sistema HANA a un grupo de recursos y realizar un backup de grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación tras fallos.

"Crear grupos de recursos y añadir políticas".

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
- Varias instancias en el mismo host
- Escalado horizontal de varios niveles replicación de sistemas HANA
- Entorno de replicación en cascada en modo de replicación de sistemas

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 Resources, haga clic en **Add SAP HANA Database**.

3. En la página Provide Resource Details, 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.
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. Para la replicación de sistemas SAP HANA, la clave de usuario secundario no está validada. Esto se utilizará durante la toma de control.
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.

No puede modificar la siguiente información si hay backups asociados con el recurso SAP HANA:

- 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.

Antes de empezar

- 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 snapshots 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.

- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "Límites de objetos para la sincronización activa de SnapMirror".

Acerca de esta tarea

- Replicación de sistemas SAP HANA
  - Puede proteger el sistema SAP HANA principal y llevar a cabo todas las operaciones de protección de datos.
  - Puede proteger el sistema SAP HANA secundario, pero no es posible crear los backups.

    Tras la conmutación al respaldo, toda la operación de protección de datos se puede realizar mientras el sistema SAP HANA secundario se convierte en el sistema SAP HANA principal.

  No puede crear un backup para el volumen de datos SAP HANA, pero SnapCenter sigue protegiendo los volúmenes no data (NDV).

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta

que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 sus detalles.
5. En la página Policy type, realice los siguientes pasos:
   - Elija el tipo de almacenamiento
   - Elija el tipo de backup:

Si desea…	Realice lo siguiente…
Crear un backup mediante la tecnología Snapshot	Seleccione **Snapshot Based**.
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.

6. En la página Snapshot and Replication, 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. 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.

7. En la página Snapshot and Replication, 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…
Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas más antiguas se eliminan primero. El valor máximo de retención es 1018. Las copias de seguridad fallarán si la retención se establece en un valor superior al que admite la versión de ONTAP . 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino. Para la replicación de sistemas SAP HANA, se recomienda añadir todos los recursos del sistema SAP HANA a un grupo de recursos. De este modo se garantiza la conservación de la cantidad adecuada de backups. Para la replicación del sistema SAP HANA, el número total de snapshots tomadas será igual a la retención establecida para el grupo de recursos. La eliminación de la copia Snapshot más antigua se basa en el nodo en el que se encuentra la copia Snapshot más antigua. Por ejemplo, la retención se establece en 7 para un grupo de recursos con la replicación de sistemas SAP HANA principal y la replicación de sistemas SAP HANA secundaria. Puede tomar un máximo de 7 Snapshots al mismo tiempo, incluyendo la replicación de sistemas SAP HANA primaria y la replicación de sistemas SAP HANA secundaria.

Si desea…	Realice lo siguiente…
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y especifique días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

8. Seleccione una etiqueta de Snapshot.

> Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

9. Para los backups basados en copias de Snapshot, en la sección Select secondary replication options, seleccione una o ambas de las siguientes opciones de replicación secundaria:

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). Esta opción debe estar habilitada para la sincronización activa de SnapMirror. Si la relación en ONTAP es del tipo Reflejo y almacén y si selecciona solo esta opción, la instancia de Snapshot creada en el origen no se transferirá al destino, pero figurará en el destino. Si esta 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. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Consulte "Consulte los backups y los clones de la base de datos SAP HANA en la página Topology".
Actualizar SnapVault después de crear una copia Snapshot local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el Almacén SnapLock, consulte "Confirmar copias Snapshot a WORM en un destino de almacén" Consulte "Consulte los backups y los clones de la base de datos SAP HANA en la página Topology".

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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

10. 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.

Acerca de esta tarea

- Para crear backups de replicación del sistema SAP HANA, se recomienda añadir todos los recursos del sistema SAP HANA a un grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación tras fallos.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admite la adición de bases de datos nuevas sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de bases de datos nuevas a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

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 los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. 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. 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 Snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

4. En la página Resources, 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 Application Settings, realice 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 **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para completar la operación de instantánea. 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 PRE y POST para las operaciones de inactividad, instantánea y desactivación. 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.
RETENCIÓN_LOG_ARCHIVO	número_de_días	Especifica la cantidad de días que se conservan los registros de archivo. 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. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.16151855 1942 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. 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 * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

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 Snapshot. En el caso de recursos de Linux, esta opción no es aplicable.	Seleccione **SnapCenter with File System Consistency**. Esta opción no es aplicable para el plugin de SnapCenter para la base de datos SAP HANA.
SnapCenter creará una snapshot a nivel del almacenamiento	Seleccione **SnapCenter sin coherencia del sistema de archivos**.
Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot.	Seleccione **Otro** y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

7. 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 + .

Las políticas figuran en la sección Configure schedules for selected policies.

b. En la columna Configure Schedules, haga clic en + en la política 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.

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. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

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

Cree grupos de recursos y habilite la protección secundaria para recursos SAP HANA en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:

a. Seleccione el tipo de política de replicación.

No se admite la política de replicación síncrona.

b. Especifique el sufijo del grupo de consistencia que desea utilizar.

c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

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.

Antes de empezar

- 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 -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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 la operación de backup basado en copias de Snapshot, asegúrese de que todas las bases de datos de tenant sean válidas y estén activas.
- Para crear backups de replicación del sistema SAP HANA, se recomienda añadir todos los recursos del sistema SAP HANA a un grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación tras fallos.

  "Crear grupos de recursos y añadir políticas".

  "Realice un backup de los grupos de recursos"

- Si desea crear un backup basado en archivos cuando una o varias bases de datos de arrendatarios están fuera de servicio, defina el parámetro ALLOW_FILE_BASED_BACKUP_IFINACTIVE_ARRENDATARIOS_PRESSE en **YES** en el archivo de propiedades de HANA mediante `Set-SmConfigSettings` cmdlet.

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

- Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y la reanudación de la copia, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin con las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

UI de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Seleccione * * y, a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede seleccionar cerrar el panel de filtros.
3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.
5. En la página Application Settings, realice lo siguiente:

   - Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales:

     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

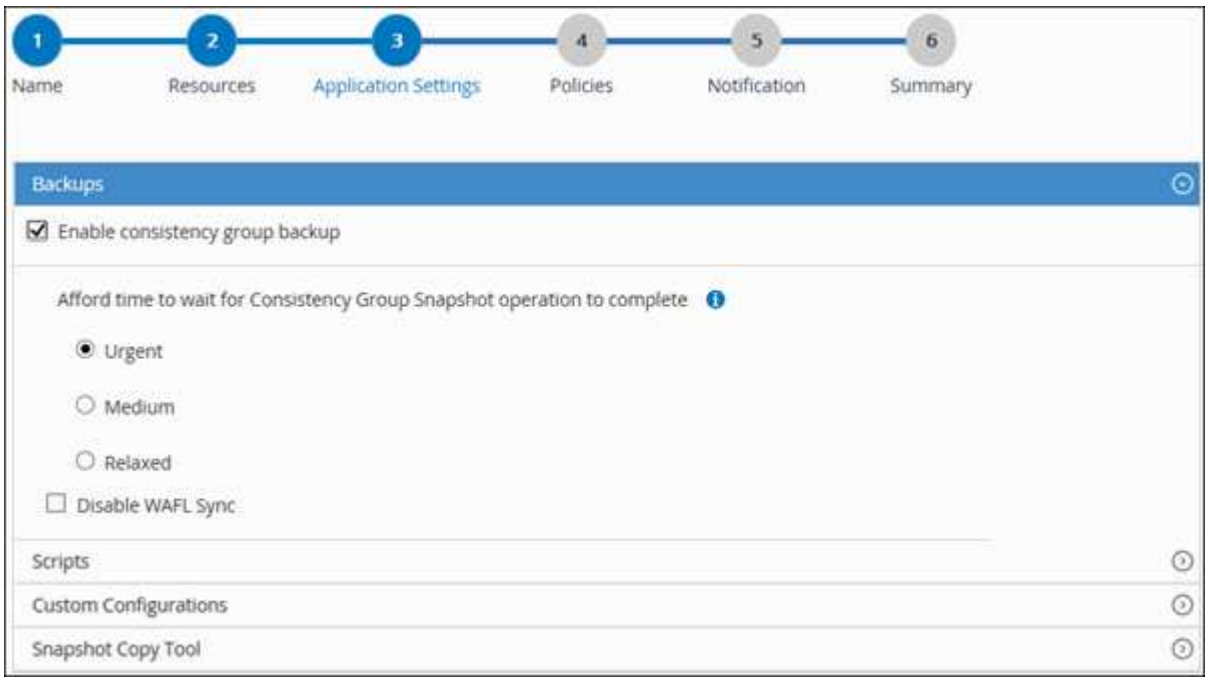
Para este campo…	**Realice lo siguiente…**
Permitir que se complete la operación de "Snapshot de grupo de consistencia"	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que finalice la operación de instantánea. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.

   - Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.

     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.
   - Seleccione la flecha **Configuraciones personalizadas**y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
   - Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	**Realice lo siguiente…**
SnapCenter cree una snapshot a 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**.
Para escribir el comando para crear una snapshot	Seleccione **Otro** y luego ingrese el comando para crear una instantánea.



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. Seleccione + en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

      policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

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. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

8. Revisa el resumen y luego selecciona **Finalizar**.

   Se muestra la página de topología de los recursos.

9. Seleccione **Back up Now**.
10. En la página Backup, 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. Seleccione **copia de seguridad**.
11. 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*

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\
   ```

   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.net
app.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"="sc
corelinux62.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";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="No
nDataVolume\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
```

6. Supervise el estado de la tarea (running, completed o failed) mediante el cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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 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, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos escribiendo su nombre en el cuadro de búsqueda o seleccionando y, luego, seleccionar la etiqueta. A continuación, puede seleccionar cerrar el panel de filtros.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **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. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Cancele las operaciones de backup para SAP HANA

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. 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 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, 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.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

- El sitio de réplica está activo.
- El sitio de réplica está inactivo.
- No se restableció la relación de reflejo o almacén secundario.

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 del número de copias de seguridad y clones disponibles en el almacenamiento principal y secundario.

   La sección **Summary Card** muestra el número total de copias de seguridad basadas en archivos, copias de seguridad basadas en copias Snapshot y clones.

   Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una

programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

- Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.
- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.

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 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.

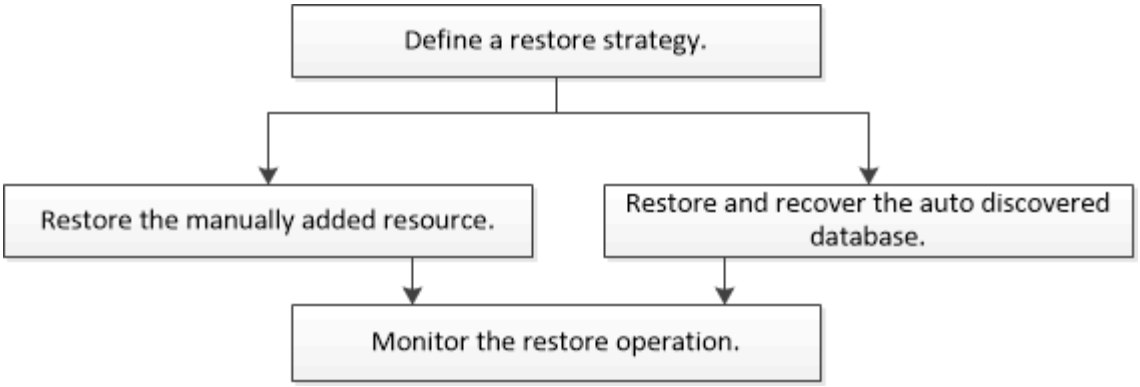
7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
8. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

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.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

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.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.

UI 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, filtre los recursos de la lista desplegable **View** 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.

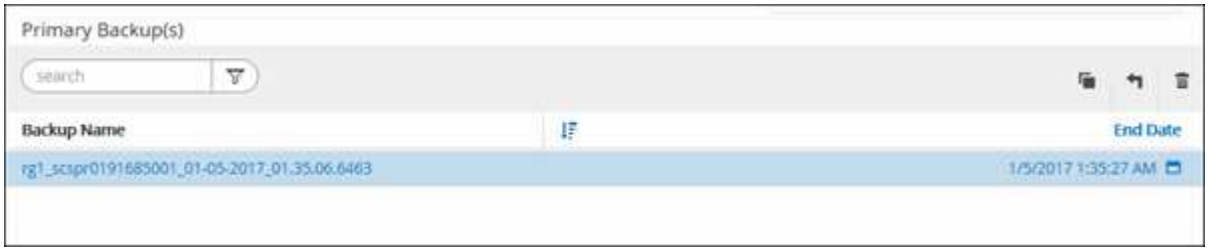
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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 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.

7. 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.

8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

9. 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 la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Restaurar y recuperar un backup de base de datos detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

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.
- Para ONTAP 9.12,1 y versiones anteriores, los clones creados a partir de las snapshots de SnapLock Vault como parte de la restauración heredarán el tiempo de caducidad del almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.

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, filtre los recursos de la lista desplegable **View** 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.

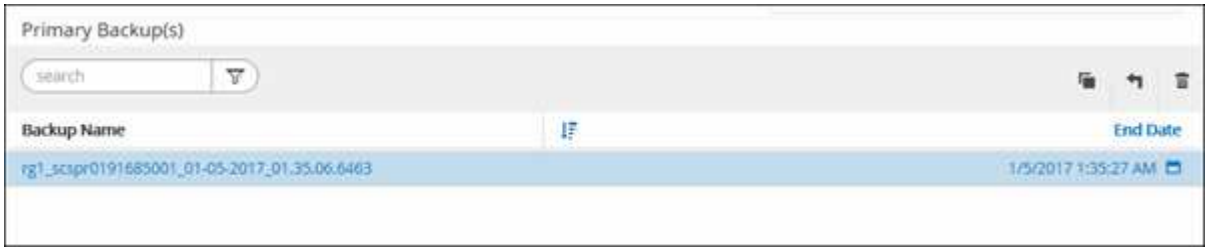
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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. 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.

7. En la página Restore Scope, 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. 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. 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**. a. Seleccione la zona horaria. De forma predeterminada, la zona horaria del navegador se completa. La zona horaria seleccionada junto con la hora de entrada se convierte en GMT absoluta. 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. 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. 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. Para los recursos de contenedor único, especifique una o más ubicaciones de backup de registro y catálogo. Para los recursos MDC, especifique una o más ubicaciones de backup de registros y la ubicación del catálogo de backups. 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.

8. 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.

9. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

10. 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 la página **Ajustes** > **Ajustes globales**.

11. Revise el resumen y, a continuación, haga clic en **Finalizar**.
12. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, 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.

Clonar backups de recursos SAP HANA

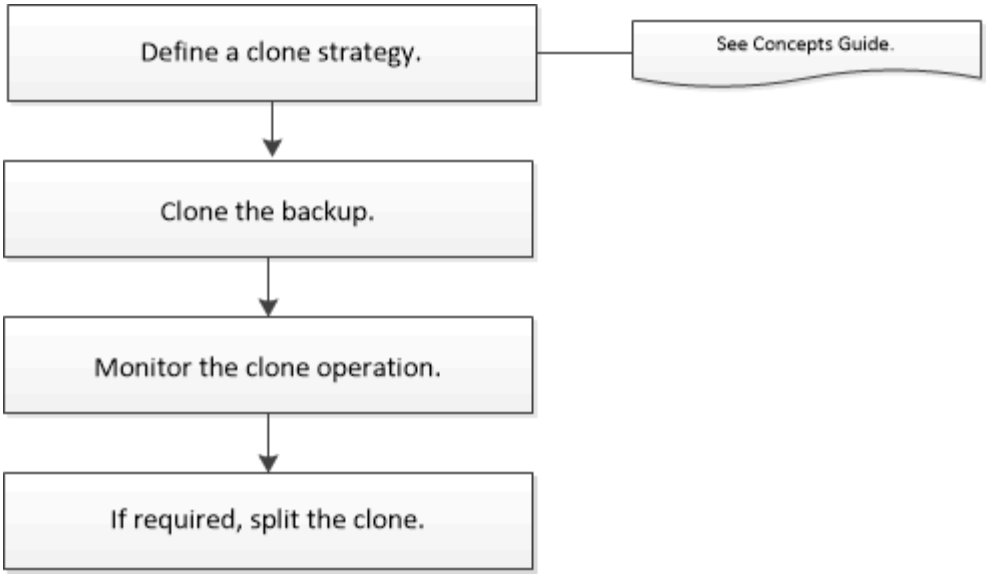
Flujo de trabajo de clonado

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.

Antes de empezar

- 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.
- Para los comandos previos o posteriores a la clonado, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Para Windows: *C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Para Linux: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Para ONTAP 9.12,1 y versiones anteriores, los clones creados a partir de las snapshots de SnapLock Vault como parte de la restauración heredarán el tiempo de caducidad del almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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 Location, lleve a cabo 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 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.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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. 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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"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 primario de la página Resources.

   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 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.
- 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

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 Snapshot de NetApp no disruptiva

  SnapCenter utiliza la tecnología 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 snapshots 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.

- Compatibilidad con la gestión de registros de archivo (ALM) para operaciones de restauración y clonado
- 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 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 del parámetro 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 el parámetro LUNPATH_MONITORING_INTERVAL. Para obtener información sobre SLM, consulte la "Sección Administración de SAN de ONTAP 9".

- Compatibilidad con memoria no volátil exprés (NVMe) en Linux
  - La utilidad NVMe debe estar instalada en el host.

    Debe instalar NVMe util para clonar o montar en un host alternativo.
  - Backup, restaurar, clonar, montar, desmontar, las operaciones de catálogo, descatalogación y verificación se admiten en el hardware de NVMe, excepto en los entornos virtualizados como RDM.

    Las operaciones anteriores se admiten en dispositivos sin particiones o con una sola partición.

    Puede configurar una solución multivía para dispositivos NVMe estableciendo la opción multivía nativa del kernel. No se admite la función multivía de Device Mapper (DM).
  - Backup, restaurar, clonar, montar, desmontar, los flujos de trabajo de catálogo, descatalogación y verificación son compatibles con NVMe over TCP/IP.
  - Backup, restaurar, clonar, montar, desmontar, los flujos de trabajo de catálogo, descatalogación y verificación se admiten en la distribución VMDK creada en NVMe over TCP/IP.
- Es compatible con la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo del sitio; es posible que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.
- Admite cualquier usuario no predeterminado en lugar de oracle y Grid.

  Para admitir los usuarios no predeterminados, debe establecer los usuarios no predeterminados modificando los valores de los parámetros en el archivo **sco.properties** ubicado en *file /var/opt/snapcenter/sco/etc/*.

  Los valores predeterminados de los parámetros se definen como oracle y GRID.
  - DB_USER=oracle
  - DB_GROUP=oinstall
  - GI_USER=cuadrícula
  - GI_GROUP=oinstall

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 • LUN conectados a iSCSI • Volúmenes conectados en NFS • NVMe-FC • NVMe/TCP
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. 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. • LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creado a través de NVMe/TCP RAC es compatible con ESX 8.0U2, que es compatible con VMDK compartido • Volúmenes NFS conectados directamente con el Guest VM • Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

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. En un entorno SAN, se admiten los sistemas de archivos ASM, LVM y SAN. No se admite NFS en AIX y sistema de archivos. • Sistema de archivos con diario mejorado (JFS2) Admite el registro en línea en sistemas DE archivos SAN y el diseño de LVM.

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para Oracle

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.

SnapCenter realiza las actualizaciones de SnapMirror y SnapVault después de completar la operación de instantánea. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter . Si está utilizando la sincronización activa de SnapMirror , utilice las programaciones predeterminadas de SnapMirror o SnapVault tanto para la sincronización activa de SnapMirror como para las relaciones asincrónicas.

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".

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.

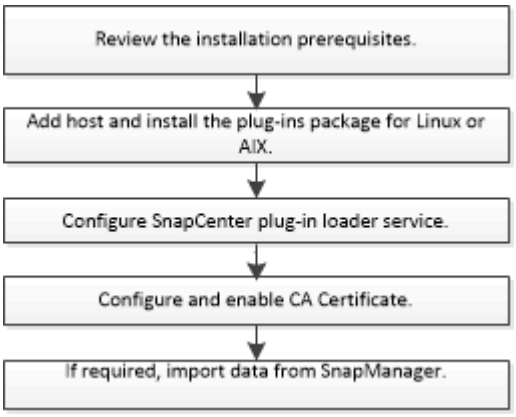
- Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - lun
  - se muestra el atributo de lun
  - lun create
  - eliminación de lun
  - geometría de lun
  - 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
  - regla adicional de la política de snapmirror
  - regla de modificación de la política de snapmirror
  - regla de eliminación de la política de snapmirror
  - la política de snapmirror
  - restauración de snapmirror
  - de snapmirror
  - historial de snapmirror
  - actualización de snapmirror
  - conjunto de actualizaciones de snapmirror
  - destinos de listas de snapmirror

- versión
- 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
- vserver
- vserver cifs
- se muestra vserver shadowcopy
- se muestra vserver
- interfaz de red
- 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 efectivo que no es raíz.

- 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 11 en el host Linux o AIX.
  - Java de Oracle y OpenJDK es compatible con Linux
  - IBM Java para AIX. Puede realizar la descarga en "Descargas de IBM Semeru Runtimes"

    Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux.

- 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.

SnapCenter no admite la asignación de UUID en el archivo /etc/fstab.

- Debe tener **bash** como shell por defecto para la instalación del plug-in.

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 • Oracle Linux 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). • SUSE Linux Enterprise Server (SLES)
RAM mínima para el plugin de SnapCenter en el host	2 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB 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	Java 11 Oracle y OpenJDK Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux. 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 la "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. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- Para el usuario que no es root, asegúrese de que el nombre del usuario que no es root y del grupo del usuario debe ser el mismo.
- 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/*LINUX_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 HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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 7,1 o posterior
RAM mínima para el plugin de SnapCenter en el host	4 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB 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 11 IBM Java 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 la "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. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- 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 HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

AIX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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. • Administrador del dominio 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: ◦ *NetBIOS\Username* ◦ *Domain FQDN\Username* • 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*
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar. 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.

Solo se admite la autenticación basada en contraseña cuando se instala el plugin en Oracle RAC. No se admite la autenticación basada en claves SSH.

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. 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.
Nombre de host	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. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • Cualquier nodo en el entorno de Oracle Real Application Clusters (RAC) El nodo VIP o IP de exploración no es compatible 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. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. 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. 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*. 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. En una configuración de Flex ASM, se agregarán todos los nodos, independientemente de si se trata de un nodo Hub o Leaf.
Omitir comprobaciones opcionales de preinstalación	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*.

resultado

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**.

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 solo se enumeren las operaciones de instalación de 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**.

Formas alternativas de instalar el paquete de plugins para Linux o AIX

También puede instalar manualmente el paquete de plugins para Linux o AIX mediante los cmdlets o CLI.

Antes de instalar el plugin manualmente, debe validar la firma del paquete binario mediante la clave **snapcenter_public_key.pub** y **snapcenter_linux_host_plugin.bin.sig** ubicado en *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Asegúrese de que **OpenSSL 1.0.2g** esté instalado en el host donde desea instalar el plugin.

Valide la firma del paquete binario ejecutando el comando:

- Para el host Linux: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Para host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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 el modo silencioso

Puede instalar el paquete de plugins de SnapCenter para Linux 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. Ejecución

     ```
     ./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.

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. Los posibles valores son TRACE, DEBUG, INFO, WARN, ERROR, Y FATAL.
SPL_PROTOCOL	Muestra el protocolo que admite el cargador del plugin de SnapCenter. 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. Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.

Nombre del parámetro	Descripción
SKIP_JAVAHOME_UPDATE	De forma predeterminada, el servicio SPL detecta la ruta de Java y el parámetro update JAVA_HOME. 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. 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. Puede agregar el valor si falta el valor predeterminado. 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.
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*. 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. Si elimina manualmente el archivo spl.properties, el número de archivos que se desea conservar se establece en 9999.

Nombre del parámetro	Descripción
JAVA_HOME	Muestra la ruta del directorio absoluto DE JAVA_HOME que se utiliza para iniciar el servicio SPL. 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. 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. 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 root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
       - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Detenga el servicio de cargador de plugins de SnapCenter:
       - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
       - Como usuario no raíz, ejecute: `sudo /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:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Busque el estado del servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
  - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Busque el cambio en el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - Como usuario no raíz, ejecute: `sudo /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.

Antes de empezar

- 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*. Alternativamente, 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 complemento SnapCenter para Oracle Database se enumeran en el siguiente documento: "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.
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. 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.

De SnapManager para Oracle y SnapManager para SAP	A SnapCenter
Configurar perfiles con Oracle Recovery Manager (RMAN)	Las directivas se crean con la opción **Catalog backup with Oracle Recovery Manager** activada. 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. 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. 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 • Lleno • SQL Server • Registro	Alcance de backup • Lleno • SQL Server • Registro	

Parámetros y valores de SnapManager para Oracle y SnapManager para SAP	Parámetros y valores de SnapCenter	Notas
Modo de backup • Automático • En línea • Sin conexión	Tipo de backup • En línea • 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 • Días • Recuentos	Retención • Días • Recuentos	SnapManager para Oracle y SnapManager para SAP utiliza tanto días como números para determinar la retención. 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 • Todo • Número de cambio de sistema (SCN) • Fecha • Registros creados antes de horas, días, semanas y meses específicos	Eliminar para programaciones • Todo • Registros creados antes de horas y días específicos	SnapCenter no admite la eliminación basada en SCN, Fecha, semanas y meses.
Notificación • Solo se envían mensajes de correo electrónico sobre operaciones desarrolladas correctamente • Solo se envían mensajes de correo electrónico sobre operaciones con errores • Se envían mensajes de correo electrónico sobre operaciones desarrolladas correctamente y operaciones con errores	Notificación • Siempre • En caso de fallo • Advertencia • Error	Las notificaciones por correo electrónico se importan. 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 su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM 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:
  - "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

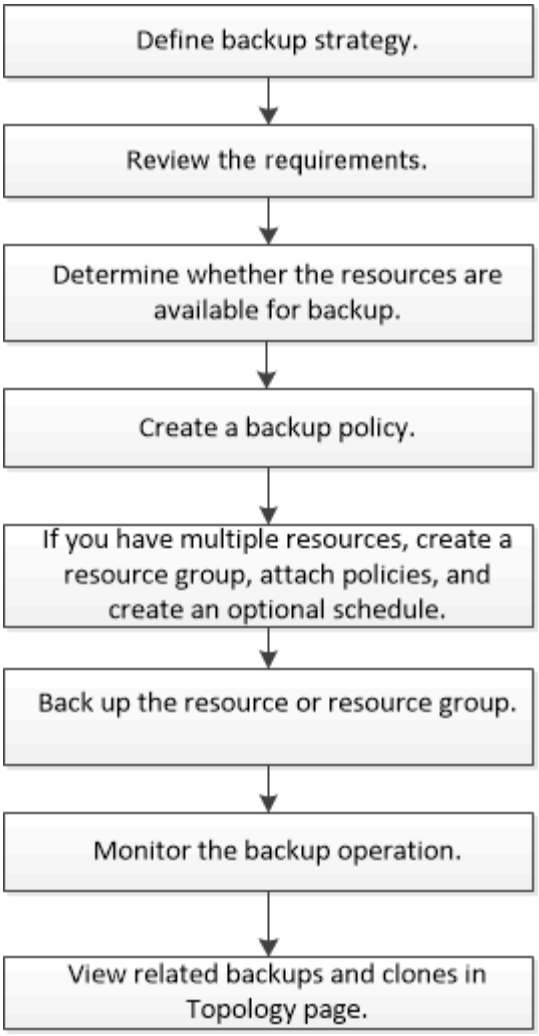
- "Documentación del plugin de SnapCenter para VMware vSphere"
- "Error en la operación de protección de datos en un entorno no multivía en RHEL 7 y versiones posteriores"

Realice backups de bases de datos de Oracle

Descripción general del procedimiento de copia de seguridad

Es posible crear un backup de un recurso (base de datos) o un grupo de recursos. El procedimiento de backup incluye planificar, identificar los recursos para el backup, crear 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:



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 */var/opt/snapcenter/sco/lock*, 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 tal situación, debe eliminar manualmente el archivo de bloqueo operativo mediante los siguientes pasos:

1. Desde el símbolo del sistema, desplácese hasta */var/opt/snapcenter/sco/lock*.
2. Elimine el bloqueo operativo:`rm -rf .sm_lock_dbsid.`

Información de configuración de backup

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 compatibles, consulte la "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

Los recursos son 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.

En las siguientes secciones se describe el proceso que utiliza SnapCenter para detectar diferentes tipos y versiones de bases de datos Oracle.

Para las versiones de Oracle 11*g* a 12*c*R1

Base de datos RAC

Las bases de datos RAC solo se detectan sobre la base de /etc/oratab`entries. Deben tener las entradas de la base de datos en el archivo /etc/oratab.

Independiente

Las bases de datos autónomas se detectan sólo sobre la base de las entradas /etc/oratab.

ASM

La entrada de instancia de ASM debe estar disponible en el archivo /etc/oratab.

RAC One Node

Las bases de datos RAC One Node sólo se detectan en función de las entradas /etc/oratab. Las bases de datos deben estar en estado nomount, mount o OPEN. Deben tener las entradas de la base de datos en el archivo /etc/oratab.

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.

Si se reubica la base de datos, debe realizar los siguientes pasos:

1. Añada manualmente la entrada de la base de datos reubicada en el archivo /etc/oratab en el nodo RAC con error.
2. Actualice manualmente los recursos.
3. Seleccione la base de datos RAC One Node en la página de recursos y, a continuación, haga clic en Database Settings.

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.
5. Ejecute las operaciones de SnapCenter.
6. Si ha reubicado una base de datos de un nodo a otro y no se ha suprimido la entrada oratab del nodo anterior, suprima manualmente la entrada oratab para evitar que se muestre la misma base de datos dos veces.

Para las versiones de Oracle 12cR2 a 18c, 19C o 21c

Base de datos RAC

Las bases de datos de RAC se detectan mediante el comando srvctl config. Deben tener las entradas de la base de datos en el archivo /etc/oratab.

Independiente

Las bases de datos independientes se detectan según las entradas en el archivo /etc/oratab y la salida del comando srvctl config.

ASM

La entrada de la instancia de ASM no debe estar en el archivo /etc/oratab.

RAC One Node

Las bases de datos RAC One Node se detectan únicamente mediante el comando srvctl config. Las bases de datos deben estar en 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.

Debe realizar los siguientes pasos si se reubica la base de datos: . Actualice manualmente los recursos. . Seleccione la base de datos RAC One Node en la página de recursos y, a continuación, haga clic en Database Settings. . Configure la base de datos para establecer los nodos de clúster preferidos en el nodo de RAC que aloja actualmente la base de datos. . 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 que utiliza SnapCenter 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 solo en estos nodos preferidos y en el orden de preferencia indicado.

Ejemplo

La base de datos de RAC cdbrac tiene tres instancias: cdbrac1 en el nodo node1, cdbrac2 en el nodo node2 y cdbrac3 en el nodo node3.

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.

Configuración de ASM Flex

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.

Base de datos de catálogo externo

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.

Comando RMAN

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 para realizar una catalogación diferida de backups `Catalog-SmBackupWithOracleRMAN` comando.

Después de catalogar los backups, es posible ejecutar el `Get-SmBackupDetails` comando para obtener la información de backups catalogados, como la etiqueta para los archivos de datos catalogados, la ruta de catálogo para el archivo de control y las ubicaciones de los registros de archivo catalogados.

Formato de nomenclatura

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.

Operaciones de verificación cruzada

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"
```

Eliminar información de catálogo

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 sobre los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help command_name. Alternativamente, puede consultar la "Guía de referencia de comandos del software SnapCenter" .

Variables de entorno predefinidas para scripts previos y posteriores específicos para backup

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y el script posterior al crear políticas de backup. Esta funcionalidad es compatible con todas las configuraciones de Oracle excepto VMDK.

SnapCenter predefine los valores de los parámetros a los que se podrá acceder directamente en el entorno en el que se ejecutan los scripts de shell. No es necesario especificar manualmente los valores de estos parámetros al ejecutar los scripts.

Variables de entorno predefinidas compatibles para crear una política de backup

- **SC_JOB_ID** especifica el ID de trabajo de la operación.

  Ejemplo: 256

- **SC_ORACLE_SID** especifica el identificador del sistema de la base de datos.

  Si la operación implica varias bases de datos, el parámetro contendrá nombres de base de datos separados por tubería.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: NFSB32|NFSB31

- **SC_HOST** especifica el nombre de host de la base de datos.

  Para RAC, el nombre de host será el nombre del host donde se realiza el backup.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** especifica el propietario del sistema operativo de la base de datos.

  Los datos se formatearán como <db1>@<osuser1>|<db2>@<osuser2>.

  Ejemplo: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** especifica el grupo de sistemas operativos de la base de datos.

  Los datos se formatearán como <db1>@<osgroup1>|<db2>@<osgroup2>.

  Ejemplo: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE**" especifica el tipo de copia de seguridad (en línea completa, datos en línea, registro en línea, apagado sin conexión, montaje sin conexión)

  Ejemplos:

  - Para una copia de seguridad completa: ONLINEFULL
  - Backup exclusivo de los datos: ONLINEDATA
  - Para copia de seguridad únicamente de registro: ONLINELOG
- **SC_BACKUP_NAME** especifica el nombre de la copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** especifica el ID de copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  EJEMPLO: DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** especifica la ruta de acceso del directorio principal de Oracle.

  Ejemplo: NFSB32@/ora01/app/oracle/product/18.1.0/dB_1|NFSB31@/ora01/app/oracle/product/18.1.0/dB_1

- **SC_BACKUP_RETENTION** especifica el período de retención definido en la directiva.

  Ejemplos:

  - Para el backup completo: Hourly|DATA@DAYS:3|LOG@COUNT:4
  - Para backup solo de datos bajo demanda: OnDemand|DATA@COUNT:2
  - Para backup solo de registros bajo demanda: OnDemand|LOG@COUNT:2
- **SC_RESOURCE_GROUP_NAME** especifica el nombre del grupo de recursos.

  Ejemplo: RG1

- **SC_BACKUP_POLICY_NAME** especifica el nombre de la política de copia de seguridad.

  Ejemplo: Backup_policy

- **SC_AV_NAME** especifica los nombres de los volúmenes de la aplicación.

  Ejemplo: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** especifica la asignación de almacenamiento de SVM al

volumen para el directorio de archivos de datos. Será el nombre del volumen principal para las lun y qtrees.

Los datos se formatearán como <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2>.

Ejemplos:

- Para 2 bases de datos en el mismo grupo de recursos: NFS32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA|NFS31@buck:/vol/sspr2417819002_NFS_CDB_NFSB31_DATA
- Para una única base de datos con archivos de datos dispersos por varios volúmenes: buck:/vol/sspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/sspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** especifica la asignación de almacenamiento de SVM al volumen para el directorio de archivos de registros. Será el nombre del volumen principal para las lun y qtrees.

  Ejemplos:

  - Para una instancia de base de datos: buck:/vol/sspr2417819002_NFS_CDB_NFSB31_REDO
  - Para varias instancias de bases de datos: NFS31@buck:/vol/sscspr2417819002_NFS_CDB_NFS31_REDO|NFS32@buck:/vol/sspr2417819002_NFS_CDB_NFS32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** especifica la lista de instantáneas que contienen el nombre del sistema de almacenamiento y el nombre del volumen.

  Ejemplos:

  - Para una única base de datos: buck:/vol/sspr2417819002_NFS_NFSB32_DATA/RG2_sspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/sspr2417819002_NFS_NFSB32_REDO/RCDB_sspr24819002_07_21_2021-02.28.26.3973--
  - Para varias instancias de bases de datos: NFS32@buck:/vol/sspr2417819002_NFS_CDB_NFS32_DATA/RG2_sspr2417819002_07-21_2021_02.28.26.3973,buck:/vol/sspr241781900_NFS_21_SCADE1900_07_2021_SCS0-B2173-B212_SCR212_02.28.26.3973_07_02.28.26.3973_SCRNFS0-B217312003-B.2_21_2021_2021_SCRNFS01.0-BC0-B.2_21_SCS01.0-B.B.2_SCR2B.B2B2B.*207*SCRSCS0-B2B2B.B.B2B2B.B.B.B.B.B.2_02.28.26.3973___
- **SC_PRIMARY_SNAPSHOT_NAMES** especifica los nombres de las instantáneas primarias creadas durante la copia de seguridad.

  Ejemplos:

  - Para una sola base de datos: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_sspr2417819002_07-21-2021_02.28.26.3973_1
  - Para varias instancias de bases de datos: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_sspr2417819002_07-21-2021_02.28.26.3973_1
  - Para instantáneas de grupo de consistencia que implican 2 volúmenes: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350
- **SC_PRIMARY_MOUNT_POINTS** especifica los detalles del punto de montaje que forman parte de la

copia de seguridad.

Los detalles incluyen el directorio en el que se montan los volúmenes, y no el primario inmediato del archivo en backup. Para una configuración de ASM, es el nombre del grupo de discos.

Los datos se formatearán como <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

Ejemplos:

- Para una única instancia de base de datos: /Mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
- Para varias instancias de bases de datos: NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/dbnfs32_log,/mnt/nfsdb32_data1
- PARA ASM: +DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** especifica los nombres de las instantáneas creadas durante la copia de seguridad de cada uno de los puntos de montaje.

  Ejemplos:

  - Para una única base de datos: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
  - Para varias instancias de bases de datos: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_data,RG2_scspr2417819002_07 02.28.26.3973-21-2021_mnt

- **SC_ARCHIVELOGS_LOCATIONS** especifica la ubicación del directorio de registros de archivo.

  Los nombres de directorio serán el primario inmediato de los archivos de registro de archivos. Si los registros de archivos se colocan en más de una ubicación, se capturarán todas las ubicaciones. Esto también incluye los escenarios de FRA. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

  - Para una única base de datos en NFS: /Mnt/nfsdb2_log
  - Para varias bases de datos en NFS y para los registros de archivo de base de datos NFSB31 que se colocan en dos ubicaciones diferentes: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
  - PARA ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** especifica la ubicación del directorio redo logs.

  Los nombres de directorio serán el primario inmediato de los archivos redo log. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

  - Para una base de datos única en NFS: /Mnt/nfsdb2_data/newdb1
  - Para varias bases de datos en NFS: NFS31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32

- PARA ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATION** especifica la ubicación del directorio de archivos de control.

  Los nombres de directorio serán el primario inmediato de los archivos de control. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

  - Para bases de datos únicas en NFS: /Mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
  - Para varias bases de datos en NFS: NFB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFB32@/mnt/nfsdb32_data/fra/dbnew32,/mnt/dbnfs32_data/newdb32
  - PARA ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS"** especifica la ubicación del directorio de archivos de datos.

  Los nombres de directorio serán el primario inmediato de los archivos de datos. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

  - Para una única base de datos en NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/DataFile
  - Para varias bases de datos en NFS: NFB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/DataFile|NFB32@/mnt/nfsdb32_data1,/mnt/dbnfs32_data/NEWDB32/DataFile
  - PARA ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE

- **SC_SNAPSHOT_LABEL** especifica el nombre de las etiquetas secundarias.

  Ejemplos: Etiqueta Hourly, Daily, Weekly, Monthly o custom.

Delimitadores compatibles

- **:** se utiliza para separar el nombre de SVM y el nombre de volumen

  Ejemplo: buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/sspr2417819002_NFS_CDB_NFSB32_REDO/RG2_sspr2417819002_07_21_2021_02.28.26.3973--

- **@** se utiliza para separar los datos de su nombre de base de datos y separar el valor de su clave.

  Ejemplos:

  - NFSB32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/sspr2417819002_NFS_sspr24B32_REDO/RCDB_sc2417875_07_21_2021_07_SCRNFS212002BS_21_02.28.26.3973_2021_02.28.26.3973_2021_07_SCNG2B2B2B2B2B2B2B2B2BV_21*02.28.26.3973SCR2BV_SCR2B2BV_SCR2BV_SCR2BSSCR24B2B2B2B2B2B2BV_*__
  - NFSB31@oracle|NFSB32@oracle

- **|** se utiliza para separar los datos entre dos bases de datos diferentes y para separar los datos entre dos entidades diferentes para los parámetros SC_BACKUP_ID, SC_BACKUP_RETENTION y SC_BACKUP_NAME.

Ejemplos:

- DATA@203|LOG@205
- HOURLY|DATA@DAYS:3|LOG@COUNT:4
- DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** se utiliza para separar el nombre del volumen de su Snapshot para SC_PRIMARY_SNAPSHOT_NAMES y los parámetros SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

  Ejemplo: NFSB32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sscspr2417819002_07-21_2021_02.28.26.3973,buck:/vol/sspr2417819002_NFS_NFSB32_REDO/RCDB_sc2417819002_07-21_2021-02.28.26.3973--

- **,** se utiliza para separar el conjunto de variables para la misma DB.

  Ejemplo: NFSB32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sspr2417819002_07-21_2021_02.28.26.3973,buck:/vol/sspr2417819002_NFS_2021_SSPR242172B_07_21_07_SCS0122B002S_21 07 02.28.26.3973_02.28.26.3973 2021 21_02.28.26.3973 2021_SCS0-B003-B003-B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2BS123-B2B2BS123-B2B2B2B2B2B2B2B2B2B2BS123-B2B2BS123-B2B2B2B2B2B2BS123-B2BS

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.

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 Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la Snapshot.

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 ms 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.

Detectar las bases de datos de Oracle 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.

Antes de empezar

- 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.

Paso 1: Evitar que SnapCenter detecte entradas que no son de base de datos

Es posible evitar que SnapCenter descubra entradas que no forman parte de una base de datos añadidas en el archivo oratab.

Pasos

1. Después de instalar el plugin para Oracle, el usuario raíz debe crear el archivo **sc_oratab.config** en el directorio */var/opt/snapcenter/sco/etc/*.

   Conceda el permiso de escritura al propietario y grupo binario de Oracle para que el archivo pueda mantenerse en el futuro.

2. El administrador de la base de datos debe añadir las entradas que no pertenecen a la base de datos en el archivo **sc_oratab.config**.

   Se recomienda mantener el mismo formato definido para las entradas que no son de base de datos en el archivo */etc/oratab* o el usuario puede añadir la cadena de entidad que no pertenece a la base de datos.

   > La cadena distingue mayúsculas de minúsculas. Cualquier texto con # en el principio se trata como un comentario. El comentario se puede agregar después del nombre que no sea de la base de datos.

   ```
   For example:
   ------------------------------------------
   # Sample entries
   # Each line can have only one non-database name
   # These are non-database name
   oratar  # Added by the admin group -1
   #Added by the script team
   NEWSPT
   DBAGNT:/ora01/app/oracle/product/agent:N
   ------------------------------------------------
   ```

3. Detectar los recursos.

   Las entradas que no sean de base de datos añadidas en **sc_oratab.config** no se mostrarán en la página Resources.

> Siempre se recomienda realizar un backup del archivo sc_oratab.config antes de actualizar el plugin de SnapCenter.

Paso 2: Descubrir recursos

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 el icono de ilter] 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 el icono imagfilter_icon.gif[filter icon]_icon.png[] 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.

Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

- 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.

Antes de empezar

- 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 snapshots 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 instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.
- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "Límites de objetos para la sincronización activa de SnapMirror".

Acerca de esta tarea

Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.

Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.

Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de SnapLock Vault como parte de la restauración heredarán el tiempo de vencimiento de SnapLock Vault. El administrador de almacenamiento debe limpiar manualmente los clones después del tiempo de vencimiento de SnapLock .

- 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 sus detalles.
6. En la página Policy type, realice los siguientes pasos:

    a. Seleccione el tipo de almacenamiento.

    b. Seleccionar ámbito de política:

        - 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.

c. 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.

d. 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.

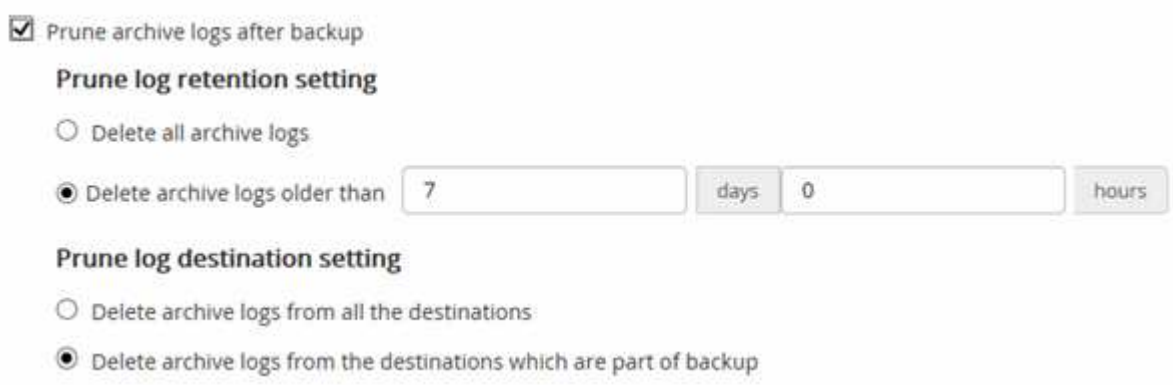
   - Puede eliminar los registros de archivos únicamente si seleccionó los archivos de registro de archivos como parte del backup.

     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.
Elimine los registros de archivos en todos los destinos	Seleccione **Eliminar registros de archivo de todos los destinos**.

Si desea…	Realice lo siguiente…
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 Snapshot and Replication, realice los siguientes pasos:

   a. 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.

   a. En la sección Data snapshot retention settings, 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…

Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas. El valor de retención máximo es 1018. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione el **Período de bloqueo de copia de instantánea** y especifique la duración en días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

b. En la sección Archive Log snapshot retention settings, 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…

Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas. El valor de retención máximo es 1018. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione el **Período de bloqueo de copia de instantánea** y especifique la duración en días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

c. Seleccione la etiqueta de política.

Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

8. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

Debe seleccionar las opciones de replicación secundarias para que el **Periodo de bloqueo de copia de instantánea secundaria** sea efectivo.

Para este campo…	Realice lo siguiente…
Actualice SnapMirror después de crear una instantánea local	Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror). Esta opción debe estar habilitada para la sincronización activa de SnapMirror. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.
Actualizar SnapVault después de crear una instantánea local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el Almacén SnapLock, consulte "Confirmar copias Snapshot a WORM en un destino de almacén" Consulte "Consulte los backups y los clones de las bases de datos de Oracle en la página Topology".
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 que se alcance el límite máximo de Snapshots 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.

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

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

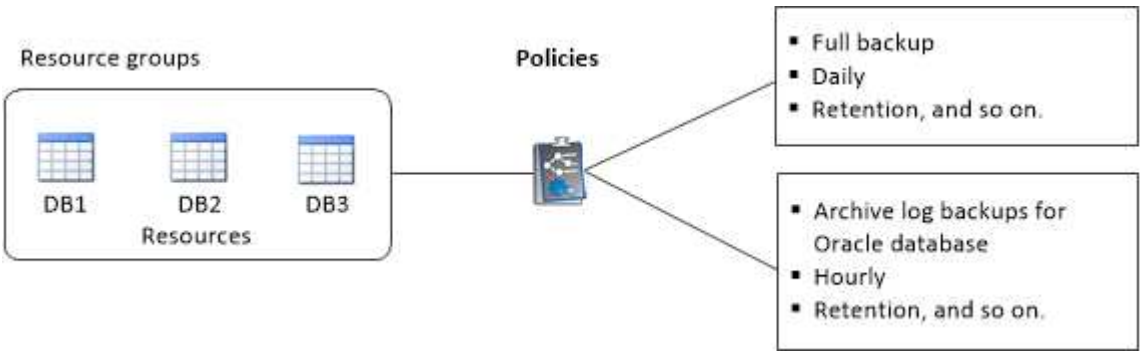
Un grupo de recursos es un contenedor donde se añaden recursos que se quieren proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación.

Acerca de esta tarea

- Una base de datos con archivos en grupos de discos de ASM debe tener el estado «MOUNT» o «OPEN» para verificar sus backups mediante la utilidad Oracle DBVERIFY.

  Añada 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:



- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admite la adición de bases de datos nuevas sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de bases de datos nuevas a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en Oracle, incluido el prefijo, si es necesario.

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 Application Settings, seleccione la opción de backup.
7. 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 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**.

   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.

8. 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.

9. 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.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Crear grupos de recursos y habilitar la protección secundaria para recursos de Oracle en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

      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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:

   a. Seleccione el tipo de política de replicación.

      No se admite la política de replicación síncrona.

   b. Especifique el sufijo del grupo de consistencia que desea utilizar.

   c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

      SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

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, seleccione **Recursos** y el plug-in apropiado de 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 de la que desea realizar el backup.

Aparece la página Database-Protect.

5. En la página Resources, realice los siguientes pasos:
   a. Marque la casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo: `customtext_policy_hostname` o. `resource_hostname`. De forma predeterminada, se añade una fecha/hora al nombre de Snapshot.

   b. 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.

      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 Configure Schedules para configurar una programación para la política que desea.
   c. En la ventana Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione `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 **Cargar localizadores** para cargar los volúmenes de SnapMirror o SnapVault para verificar 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. + En el cuadro de diálogo Add Verification Schedules *policy_name*, puede realizar los siguientes pasos:
   c. Seleccione **Ejecutar verificación después de la copia de seguridad**.
   d. Seleccione **Ejecutar verificación programada** y seleccione el tipo de programación en la lista desplegable.

      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.

   e. Seleccione **verificar en la ubicación secundaria** para verificar las copias de seguridad en el almacenamiento secundario.
   f. Haga clic en **Aceptar**.

      Las programaciones de verificación configuradas aparecerán en la columna Applied Schedules.
8. En la página Notificación, seleccione los escenarios en los que desea enviar los correos electrónicos desde la lista desplegable **Preferencias de correo electrónico**.

   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 el comando de PowerShell `Set-SmSmtpServer`.

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

   Se muestra la página de topología de la base de datos.

10. Haga clic en **copia de seguridad ahora**.
11. 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**.
12. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

- En la configuración de AIX, puede utilizar `lkdev` comando para bloquear y el `rendev` comando para cambiar el nombre de los discos en los que residía la base de datos de la que se realizó un backup.

  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 debido a que el tiempo de ejecución de la consulta de base de datos superó el valor del tiempo de espera, debe cambiar el valor de los parámetros ORACLE_SQL_QUERY_TIMEOUT y ORACLE_PLUGIN_SQL_QUERY_TIMEOUT mediante la ejecución del `Set-SmConfigSettings` cmdlet:

  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`.

Obtenga 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" (Requiere inicio de sesión)

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. La operación de backup se realiza con todos los recursos definidos en el grupo de recursos.

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si el grupo de recursos tiene una política anexada y una programación configurada, los backups se crean según esa programación.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. Escriba el nombre del grupo de recursos en el cuadro de búsqueda o haga clic en y seleccione la etiqueta.

   Haga clic en para cerrar el panel de filtros.

4. En la página Resource Group, seleccione el grupo de recursos que desea incluir en un backup.

   Si posee un grupo de recursos federado con dos bases de datos y una tiene datos en un almacenamiento de terceros, se cancelará la operación de backup aunque la otra base de datos esté en almacenamiento de NetApp.

5. En la página Backup, realice los siguientes pasos:
   a. Si tiene varias políticas asociadas con el grupo de recursos, seleccione la política de copia de seguridad que desea usar en la lista desplegable **Política**.

      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 **copia de seguridad**.
6. Controla el progreso seleccionando **Monitor > Trabajos**.

Después de terminar

- En la configuración de AIX, puede utilizar `lkdev` comando para bloquear y el `rendev` comando para cambiar el nombre de los discos en los que residía la base de datos de la que se realizó un backup.

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 debido a que el tiempo de ejecución de la consulta de base de datos superó el valor del tiempo de espera, debe cambiar el valor de los parámetros ORACLE_SQL_QUERY_TIMEOUT y ORACLE_PLUGIN_SQL_QUERY_TIMEOUT mediante la ejecución del `Set-SmConfigSettings` cmdlet:

  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`

Supervisar la copia de seguridad de Oracle Database

Descubra cómo supervisar el progreso de las operaciones de backup y las operaciones de protección de datos.

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Otras operaciones de backup

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 sobre los parámetros que se pueden utilizar con el comando y sus descripciones se pueden obtener ejecutando Get-Help *command_name*. Alternativamente, 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*

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 snapshots del almacenamiento si el backup creado no se registró en el servidor de SnapCenter. Si la copia de seguridad ya está registrada en el servidor de SnapCenter, no revertirá la copia 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**. 2. Seleccione la operación y haga clic en **Cancelar trabajo**.
Panel de actividades	1. Después de iniciar la tarea de backup, haga clic en en el panel Activity para ver las cinco operaciones más recientes. 2. Seleccione la operación. 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.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

- El sitio de réplica está activo.
- El sitio de réplica está inactivo.
- No se restableció la relación de reflejo o almacén secundario.
- 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.

     Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario

recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

- Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.
- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.

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*.

Alternativamente, 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
  - En NVMe, se debe instalar NVMe util
- 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 sobre los parámetros que se pueden utilizar con el comando y sus descripciones se pueden obtener ejecutando Get-Help *command_name*. Alternativamente, 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 .

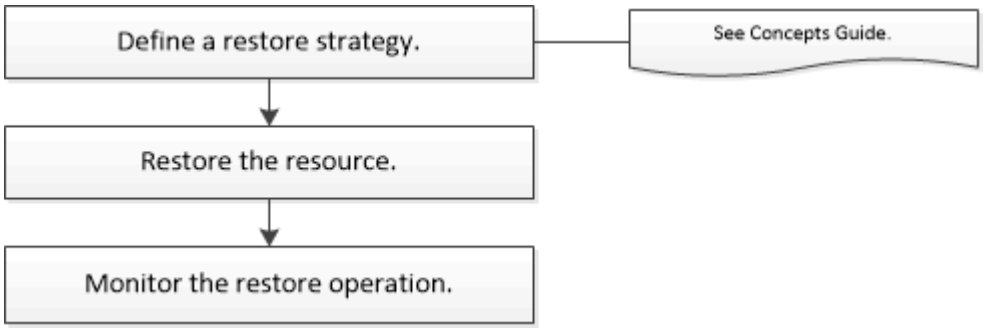
5. Haga clic en **Aceptar**.

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

> Si va a restaurar un backup de datos sin conexión apagado o sin conexión montado, SnapCenter deja la base de datos en estado sin conexión. Es necesario recuperar manualmente la base de datos y restablecer los registros.

- 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
- 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.

NetApp ONTAP es compatible 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 archivos temporales porque el complemento para Oracle no realiza copias de seguridad de los archivos temporales.
- 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.

Variables de entorno predefinidas para restaurar scripts previos y posteriores específicos

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y el script posterior mientras se restaura una base de datos.

Variables de entorno predefinidas admitidas para restaurar una base de datos

- **SC_JOB_ID** especifica el ID de trabajo de la operación.

  Ejemplo: 257

- **SC_ORACLE_SID** especifica el identificador del sistema de la base de datos.

  Si la operación implica varias bases de datos, esto contendrá nombres de bases de datos separados por tuberías.

  Ejemplo: NFSB31

- **SC_HOST** especifica el nombre de host de la base de datos.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

Ejemplo: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** especifica el propietario del sistema operativo de la base de datos.

  Ejemplo: oracle

- **SC_OS_GROUP** especifica el grupo de sistemas operativos de la base de datos.

  Ejemplo: Oinstall

- **SC_BACKUP_NAME** especifica el nombre de la copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplos:

  - Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Si la base de datos se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21-2021_12.16.48.9267_1,RG2_sspr2417819002_07-22-2021_12.16.48.9267_1

- **SC_BACKUP_ID** especifica el ID de la copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplos:

  - Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@203|LOG@205
  - Si la base de datos se está ejecutando en modo ARCHIVELOG: DATA@203|LOG@205,206,207

- **SC_RESOURCE_GROUP_NAME** especifica el nombre del grupo de recursos.

  Ejemplo: RG1

- **SC_ORACLE_HOME** especifica la ruta de acceso del directorio principal de Oracle.

  Ejemplo: /Ora01/app/oracle/product/18.1.0/dB_1

- **SC_RECOVERY_TYPE** especifica los archivos que se recuperan y también el ámbito de recuperación.

  Ejemplo: RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Para obtener más información acerca de los delimitadores, consulte "Delimitadores compatibles".

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 Snapshots 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 y recuperar bases 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.

Antes de empezar

Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.

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 la base de datos se está ejecutando en modo ARCHIVELOG, Oracle Database guarda los grupos rellenados de archivos redo log en uno o más destinos sin conexión, conocidos conjuntamente como redo log archivado. SnapCenter identifica y monta la cantidad óptima de backups de registros según el SCN especificado, la fecha y la hora seleccionadas o la opción All logs.
  Si los registros de archivos necesarios 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 archivos 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 */var/opt/snapcenter/sco/lock*, 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.

- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- 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**. 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**. Se pueden especificar los espacios de tabla que se desean restaurar.
Archivos de control	Seleccione **Archivos de control**. 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**. Esta opción está disponible solo para bases de datos Data Guard en espera o Active Data Guard en espera. 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.

Si desea restaurar…	Realice lo siguiente…
Bases de datos conectables (PDB)	Seleccione **Pluggable databases** y, a continuación, especifique las PDB que desea restaurar.
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. 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**. 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	Si la base de datos se ejecuta en modo ARCHIVELOG, SnapCenter identifica y monta el número óptimo de backups de registros según el SCN especificado, la fecha y la hora seleccionadas o la opción All logs. Si aún desea especificar la ubicación de los archivos de registro de archivos externos, seleccione **especificar ubicaciones de registro de archivos externos**. 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. Debe verificar la ruta y el contenido de la ruta de montaje antes de enumerarla como ubicación de registro externo. • "Protección de datos de Oracle con ONTAP" • "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.

   SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y script

posterior. "Leer más"

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.

      Si se produce un error en la operación de restauración, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

   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.

Antes de empezar

- Los backups necesarios para ejecutar PITR de espacios de tablas deben catalogarse y montarse.
- Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.

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.

     SnapCenter identifica y, a continuación, monta y cataloga la cantidad óptima de backups de datos y registros necesarios para realizar PITR según el SCN especificado o la fecha y hora seleccionadas.

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.

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

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.

      Si se produce un error en la operación de restauración, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

   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.

Antes de empezar

- 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.

- Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.

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)**. ii. Especifique la PDB que desea restaurar. 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)**. ii. Especifique la PDB. iii. Especifique un único espacio de tabla o varios espacios de tablas que desee 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.

     SnapCenter identifica y, a continuación, monta y cataloga la cantidad óptima de backups de datos y registros necesarios para realizar PITR según el SCN especificado o la fecha y hora seleccionadas.

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.

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

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.

      Si se produce un error en la operación de restauración, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

   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 sobre los parámetros que se pueden utilizar con el comando y sus descripciones se pueden obtener ejecutando Get-Help *command_name*. Alternativamente, también puede consultar la "Guía de referencia de comandos del software SnapCenter" .

- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.
- 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.

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

- Puede cancelar una operación de restauración en cola desde la página **Monitor** o desde el panel **actividad**.
- 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**. 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. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**.

Clone la base de datos de Oracle

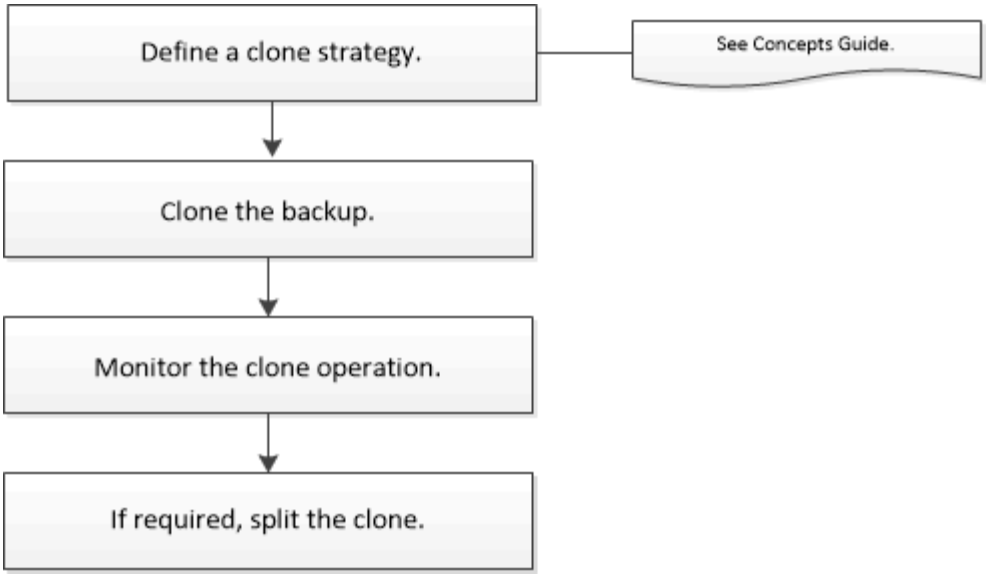
Flujo de trabajo de clonado

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

> Las configuraciones DE SAN no son compatibles si la opción USER_Friendly_Names del archivo de configuración multivía está establecida en yes.

> 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.

Variables de entorno predefinidas para el script previo y script posterior específicos de clon

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y el script posterior mientras se clona una base de datos.

Variables de entorno predefinidas admitidas para clonar una base de datos

- **SC_ORIGINAL_SID** especifica el SID de la base de datos de origen.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: NFSB32

- **SC_ORIGINAL_HOST** especifica el nombre del host de origen.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** especifica la ruta de acceso del directorio raíz de Oracle de la base de datos de destino.

  Ejemplo: /Ora01/app/oracle/product/18.1.0/dB_1

- **SC_BACKUP_NAME**" especifica el nombre de la copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplos:

  - Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Si la base de datos se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_sscspr2417819002_07-20-2021_12.16.48.9267_1,RG2_sspr2417819002_07-21-2021_12.16.48.9267_1,RG2_sspr2417819002_07-22-2021_12.16.48.9267_1

- **SC_AV_NAME** especifica los nombres de los volúmenes de la aplicación.

  Ejemplo: AV1|AV2

- **SC_ORIGINAL_OS_USER** especifica el propietario del sistema operativo de la base de datos de origen.

  Ejemplo: oracle

- **SC_ORIGINAL_OS_GROUP** especifica el grupo de sistemas operativos de la base de datos de origen.

  Ejemplo: Oinstall

- **SC_TARGET_SID**" especifica el SID de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: Clonedb

- **SC_TARGET_HOST** especifica el nombre del host donde se clonará la base de datos.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: asmrac1.gdl.englab.netapp.com

- **SC_TARGET_OS_USER** especifica el propietario del sistema operativo de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Ejemplo: oracle

- **SC_TARGET_OS_GROUP** especifica el grupo del sistema operativo de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Ejemplo: Oinstall

- **SC_TARGET_DB_PORT** especifica el puerto de base de datos de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Ejemplo: 1521

Para obtener más información acerca de los delimitadores, consulte "Delimitadores compatibles".

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.

    - En NVMe, se debe instalar NVMe util
- 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 el backup 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).
- Para NVMe, si debe excluir un puerto de destino de la conexión, debe añadir el nombre del nodo de destino y el nombre del puerto en el archivo /var/opt/snapcenter/scu/etc/nvme.conf.

  Si el archivo no existe, debe crearlo como se muestra en el siguiente ejemplo:

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- 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.

Antes de empezar

Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.

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 la cantidad óptima de backups de registros basados en SCN o dat y el tiempo 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.

- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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. El SID del clon no está disponible de manera predeterminada, y la longitud máxima del SID es de 8 caracteres. 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**. b. Especifique la PDB que desea clonar. 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. 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. La convención de nomenclatura predeterminada de SnapCenter para sistemas de archivos SAN o NFS es FileSystemNameofsourcedatabase_CLONESID. 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. Si personaliza el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre respete el límite admitido por Oracle. 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. 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. El sistema de archivos o el grupo de discos ASM deben existir en el host. 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. 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. 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. El nuevo sistema de archivos o el grupo de discos ASM deben existir en el host. 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: • Cantidad de grupos de registros de recuperación Se requiere un mínimo de dos grupos de registros de recuperación para clonar la base de datos. • Los archivos de registro de recuperación en cada grupo y su ruta de acceso 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. Se requiere un mínimo de un archivo de registro de recuperación en el grupo de registros de recuperación para clonar la base de datos. • 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. 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. 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.

      SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

   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.

      Puede agregar parámetros adicionales haciendo 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 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	Si la base de datos se ejecuta en modo ARCHIVELOG, SnapCenter identifica y monta el número óptimo de backups de registros según el SCN especificado o la fecha y hora seleccionadas. También es posible especificar la ubicación del registro de archivos externo. SnapCenter no identifica ni monta automáticamente los backups de registros si seleccionó hasta Cancel.
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. 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. 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.

Nombre del campo	Descripción
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. 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*. 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. Si se produce un error en la operación de clonado, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

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.

12. 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.

13. 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"

Actualice la IP preferida en el host

Una vez completada la operación de clonado, la ruta que proporciona la capa de acceso a almacenamiento (SAL) al clon tendrá el formato *<nfs_lif_IP>:<JunctionPath>*. Para proporcionar la IP preferida, debe configurarla en el host mediante los comandos SCCLI.

Pasos

1. Conéctese al host de la base de datos.
2. Inicie una sesión de conexión de PowerShell con SnapCenter, para el usuario especificado.

   Open-SmConnection

3. Cree un archivo vacío.

   toque /var/opt/SnapCenter/scu/etc/storagepreference.properties

4. Configure la LIF de datos preferida para la SVM.

   Add-SvmPreferredDataPath -SVM <SVM Name> -DataPath <dirección IP o FQDN>

5. Compruebe la ruta preferida.

   Get-SvmPreferredDataPath

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.

Antes de empezar

Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.

- 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 los siguientes pasos:
   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. 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. 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. La convención de nomenclatura predeterminada de SnapCenter para sistemas DE archivos SAN o NFS es FileSystemNameofsourcedatabase_SCJOBID. 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. Si personaliza el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre respete el límite admitido por Oracle. 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.

   SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

   a. 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. 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. 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. 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.

Nombre del campo	Descripción
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. 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. 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*. 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. Si se produce un error en la operación de clonado, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

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 sobre los parámetros que se pueden utilizar con el comando y sus descripciones se pueden obtener ejecutando Get-Help *command_name*. Alternativamente, 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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal"
- 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 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 los comandos de UNIX, consulte la "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 PDB (targetCDB:PDBClone) y, a continuación, haga clic en .

5. Haga clic en **Aceptar**.

Gestione los volúmenes de aplicaciones

¿Qué son volúmenes de aplicación

Los volúmenes de aplicaciones son el almacenamiento donde se almacena información como la configuración, el instalador y otros archivos que no son de datos relacionados con la base de datos Oracle.

El plugin de SnapCenter para bases de datos de Oracle permite crear un backup consistente de volúmenes de aplicaciones (no volúmenes de datos) junto con las bases de datos de Oracle.

El complemento automatiza el backup y la clonado de volúmenes de aplicaciones.

- Proteja los volúmenes de aplicaciones junto con los volúmenes de bases de datos de Oracle en un único grupo de recursos.
- Crear backups de volúmenes de aplicaciones.
- Crear backups de bases de datos de Oracle junto con volúmenes de aplicación.
- Crear clones de bases de datos junto con volúmenes de aplicaciones hasta un momento específico.
- Programar operaciones de backup.
- Supervisar todas las operaciones.
- Ver informes de operaciones de backup y clonado.

Añada volúmenes de la aplicación

SnapCenter permite realizar backups y clonado de volúmenes de aplicaciones de bases de datos de Oracle. Debe añadir manualmente los volúmenes de la aplicación. No se admite la detección automática de volúmenes de aplicaciones.

Los volúmenes de aplicaciones solo admiten conexiones iSCSI directas y NFS.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. Haga clic en **Agregar volumen de aplicación**.
  3. En la página Name, realice los siguientes pasos:
     - En el campo Name, introduzca el nombre del volumen de la aplicación.
     - En el campo Host Name, introduzca el nombre del host.
  4. En la página Huella de almacenamiento, realice las siguientes acciones:
     - Seleccione el tipo de almacenamiento.
     - Introduzca el nombre del sistema de almacenamiento.
     - Seleccione las unidades de almacenamiento.

       Puede agregar varias unidades de almacenamiento.

5. Revise el resumen y, a continuación, haga clic en **Finalizar**.
6. En la página Resources, seleccione **volumen de aplicación** en la lista **View** para ver todos los volúmenes de aplicación que ha agregado.

Modifique el volumen de la aplicación

Es posible modificar todos los valores especificados al añadir el volumen de aplicaciones si no se crean backups. Si se crea el backup, solo puede modificar los detalles del sistema de almacenamiento.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Haga clic en para modificar los valores.
  4. Haga clic en para modificar los valores.

Elimine el volumen de la aplicación

Cuando se elimina un volumen de aplicaciones, si hay backups asociados con el volumen de la aplicación, el volumen se pondrá en modo de mantenimiento y no se crearán backups nuevos y no se conservarán backups anteriores. Si no hay backups asociados, se eliminan todos los metadatos.

Si es necesario, SnapCenter permite deshacer la operación de eliminación.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Hacer clic para eliminar el volumen de la aplicación.

Aplicación de backup para volúmenes

Realice un backup del volumen de la aplicación

Si el volumen de la aplicación no forma parte de ningún grupo de recursos, es posible realizar backups del volumen de la aplicación desde la página Resources.

Acerca de esta tarea

De manera predeterminada, se crean backups de grupo de consistencia (CG). Si desea crear copias de seguridad basadas en volúmenes, debe establecer el valor de **EnableOracleNdvVolumeBasedBackup** en true en el archivo *web.config*.

- Pasos*

  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.

2. En la página Resources, seleccione **volumen de aplicación** 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 el volumen de la aplicación del que desea realizar un backup.

   Aparece la página Application volume-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 y después introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot. Por ejemplo, customtext__policy_hostname o resource_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la 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.

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. Se debe hacer clic en en la columna Configure Schedules para la política cuya programación se desea configurar.

   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 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 del volumen de la aplicación.

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.
   b. Haga clic en **copia de seguridad**.
4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Realice un backup del grupo de recursos de volúmenes de aplicaciones

Es posible realizar un backup del grupo de recursos que solo contenga volúmenes de aplicación o una combinación de volúmenes de aplicaciones y bases de datos. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Si el grupo de recursos tiene varios volúmenes de aplicaciones, todos los volúmenes de aplicaciones deben tener una política de replicación de SnapMirror o SnapVault.

Acerca de esta tarea

De manera predeterminada, se crean backups de grupo de consistencia (CG). Si desea crear copias de seguridad basadas en volúmenes, debe establecer el valor de **EnableOracleNdvVolumeBasedBackup** en true en el archivo *web.config*.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database 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, luego, 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 de la operación haciendo clic en **Monitor** > **Jobs**.

Se realizará la operación de verificación solo para las bases de datos y no para los volúmenes de aplicaciones.

Clone el backup de volumen de la aplicación

Es posible utilizar SnapCenter para clonar los backups de volumen de aplicaciones.

Antes de empezar

Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
3. Seleccione el volumen de la aplicación en la vista de detalles del volumen de la aplicación o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología del volumen de la aplicación.

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 Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Host de plugin	Seleccione el host donde desea crear el clon.
Nombre del recurso de destino	Especifique el nombre del recurso.

7. En la página Scripts, especifique los nombres de los scripts que se van a ejecutar antes de la clonación, comandos para montar un sistema de archivos y nombres de los scripts que se van a ejecutar después de la clonación.
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 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**.

Divida un clon de volumen de aplicación

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Seleccione el recurso clonado 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**.

Eliminar un clon de volumen de aplicaciones

Puede eliminar clones si ya no le resultan necesarios. No puede eliminar clones que actúan como origen para otros clones.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **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 .
  6. En la página Delete Clone, lleve a cabo las acciones siguientes:
     a. En el campo **Pre clone delete**, introduzca los nombres de las secuencias de comandos que se van a ejecutar antes de eliminar el clon.
     b. En el campo **Unmount**, introduzca los comandos para desmontar el clon antes de eliminarlo.
  7. 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 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.

- 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 coherencia 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.

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 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 NetApp instantánea no disruptiva**

  El plugin para Windows utiliza la tecnología 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 snapshots 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
- Compatibilidad con memoria no volátil rápida (NVMe) en Windows Server 2022
  - Flujos de trabajo de backup, restauración, clonado y verificación en distribución de VMDK creada en NVMe over TCP/IP.
  - Es compatible con la versión de firmware 1,3 de NVMe a partir de la actualización 2 de ESX 8,0 y

requiere la versión 21 de hardware virtual.

    - No se admite Windows Server Failover Clustering (WSFC) para aplicaciones a través de VMDK en NVMe sobre TCP/IP.
    - Las controladoras NVMe solo son compatibles con los datastores NVMe.

- Es compatible con la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo del sitio; es posible que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.

Cómo hace SnapCenter para realizar backup de sistemas de archivos Windows

SnapCenter usa la tecnología 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 snapshots 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 snapshot del volumen, en lugar de Snapshots individuales de cada sistema de archivos.

Cuando SnapCenter crea una copia Snapshot, se captura todo el volumen del sistema de almacenamiento en la copia 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 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 el plugin 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.

El soporte de aprovisionamiento y protección de datos de SnapCenter está disponible en Windows Server. Para obtener la información más reciente sobre las versiones compatibles, consulte la "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.
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.
Máquina virtual de VMware	Almacenes de datos VVOL en NFS y SAN	Herramientas de ONTAP para VMware vSphere	

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. 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. 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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
    - 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 8.3.0 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.

SnapCenter realiza las actualizaciones de SnapMirror y SnapVault después de completar la operación de instantánea. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter . Si está utilizando la sincronización activa de SnapMirror , utilice las programaciones predeterminadas de SnapMirror o SnapVault tanto para la sincronización activa de SnapMirror como para las relaciones asincrónicas.

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 de Snapshot predeterminada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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.

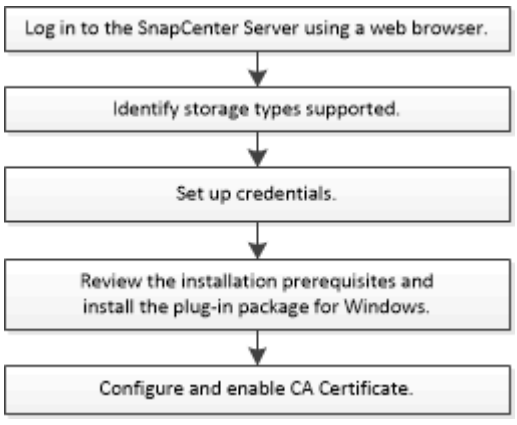
Destino de clones	Descripción
Original, origen, ubicación	De forma predeterminada, SnapCenter almacena el clon en la misma ubicación y el mismo host que el backup que se clona.
Otra ubicación	Es posible almacenar el clon en otra ubicación en el mismo host o en otro. El host debe tener una conexión configurada 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 Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Si está en una configuración de clúster de Windows, también debe instalar y configurar la Administración remota de Windows (WinRM).
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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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. • 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 Username son los siguientes: ◦ `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 el siguiente: `UserName` 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 un grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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 2016 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
- 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.

SnapCenter no admite la adición de un mismo host (host del plugin) a SnapCenter si el host ya forma parte de un grupo de trabajo y se cambió a otro dominio o viceversa.
Si desea añadir el mismo host, debe quitar el host de SnapCenter y volver a añadirlo.

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**. El servidor de SnapCenter añade el host y, a continuación, instala el plugin para Windows si aún no está instalado 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. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el nombre de dominio completamente cualificado (FQDN). Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • Clustering de conmutación al nodo de respaldo de Windows Server (WSFC) 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. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte los detalles de cómo crear una credencial. 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. 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. 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. 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. 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. Proporcione el nombre de GMSA con el siguiente formato: *Domainname\accountName$*. 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.

8. 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*. Alternativamente, 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.

Antes de empezar

- Debe haber instalado ASP.NET Core Runtime 8.0.12 (y todos los parches posteriores de 8,0.x) Hosting Bundle.

- Debe haber instalado PowerShell 7.4.2 o posterior.
- 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.
SUITE_INSTALLDIR	Indique el directorio de instalación para el paquete de plugins del host.

Variable	Valor
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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$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.

Antes de empezar

- 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*. Alternativamente, 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 su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM 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.

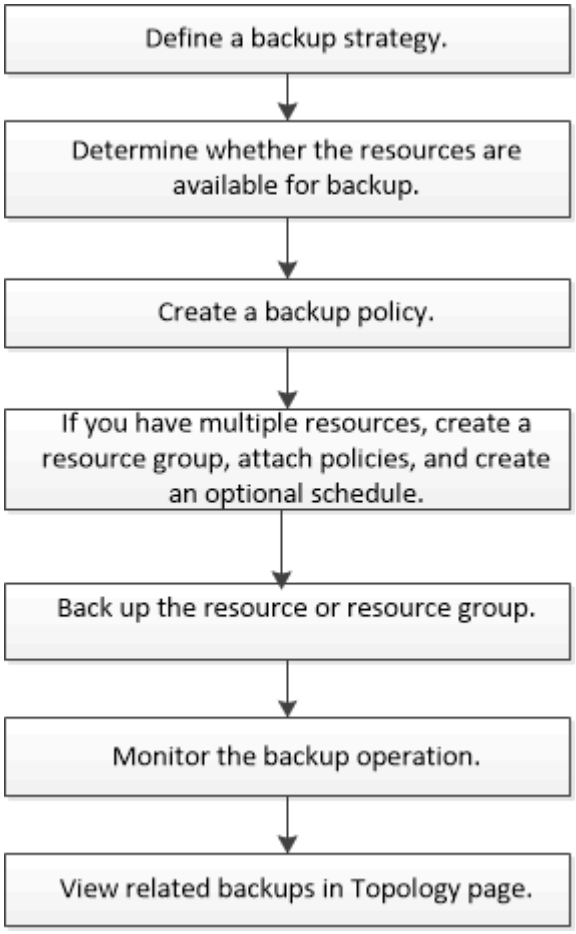
Realizar backup de sistemas de archivos Windows

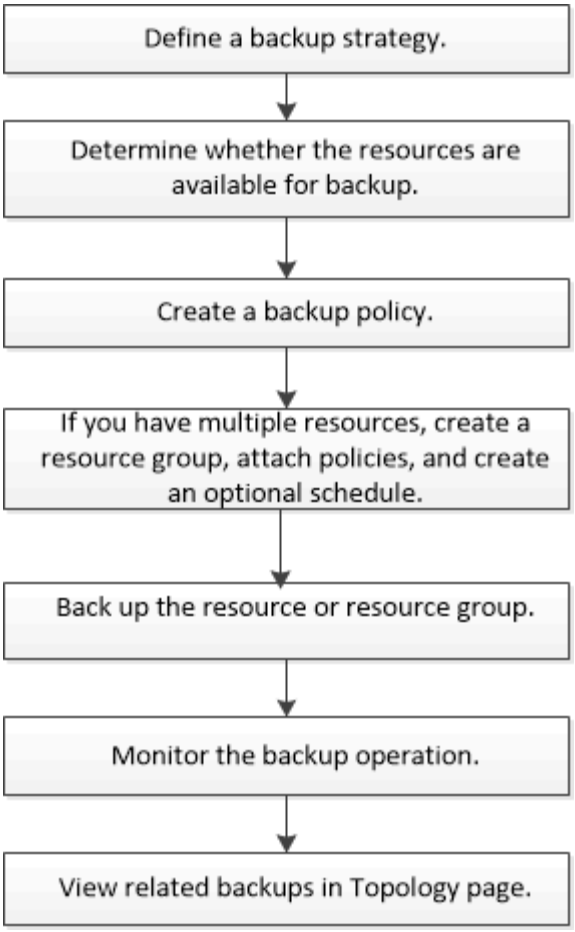
Realizar backup de sistemas de archivos Windows

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 sobre cmdlet de SnapCenter y el "Guía de referencia de cmdlets de SnapCenter Software" contienen 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.

Antes de empezar

- 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.

   Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

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.

Antes de empezar

- 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 snapshots 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

- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "Límites de objetos para la sincronización activa de SnapMirror".

Acerca de esta tarea

- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.
  - Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén

de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

Pasos

1. En el panel de navegación izquierdo, selecciona **Configuración**.
2. En la página Configuración, selecciona **Políticas**.
3. Selecciona **Nuevo**.
4. En la página Name, escriba el nombre de la política y sus detalles.
5. En la página Backup and Replication, 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.

   c. Seleccione una etiqueta de política.

   Según la etiqueta de Snapshot que seleccione, ONTAP aplicará la política de retención de Snapshot secundaria que corresponda a esa etiqueta.

   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.

6. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

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). Esta opción debe estar habilitada para la sincronización activa de Snapmirror. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Consulte "Consulte los backups y los clones relacionados en la página Topology".
Actualizar SnapVault después de crear una copia Snapshot	Seleccione esta opción para realizar una replicación de backup de disco a disco. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón Refresh de la página Topology, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recupera de ONTAP. Cuando SnapLock se configura solo en el secundario de ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón Actualizar de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el Almacén SnapLock, consulte "Confirmar copias Snapshot a WORM en un destino de almacén"
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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

7. En la página Retention settings, especifique la configuración de retención para backups bajo demanda y para cada frecuencia de programación que seleccionó.

Opción	Descripción
Copias de Snapshot totales que se deben conservar	Elija esta opción si desea especificar el número de instantáneas que SnapCenter almacena antes de eliminarlas automáticamente.
Conserve copias Snapshot para	Elija esta opción si desea especificar el número de días que SnapCenter retiene una copia de backup antes de eliminarla.
Período de bloqueo de copia de instantánea	Seleccione el período de bloqueo de la instantánea y especifique la duración en días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

Debe establecer el número de retención en 2 o superior. El valor mínimo para el número de retención es 2.

El valor máximo de retención es 1018. Las copias de seguridad fallarán si la retención se establece en un valor superior al que admite la versión de ONTAP .

8. 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.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

9. 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.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admiten la adición de sistemas de archivos nuevos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de sistemas de archivos nuevos a un grupo de recursos existente en el modo de

conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

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. El nombre del grupo de recursos no debe superar los 250 caracteres.
Utilice un formato de nombre personalizado para la copia de Snapshot	Opcional: Introduzca un nombre y un formato de Snapshot personalizados. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la 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.

b. 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.

c. Si la política está asociada con varios tipos de programación (frecuencias), seleccione la frecuencia que desea configurar.

d. 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.

7. 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

8. 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.

Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Windows en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

      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.
8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:
   a. Seleccione el tipo de política de replicación.

      No se admite la política de replicación síncrona.

   b. Especifique el sufijo del grupo de consistencia que desea utilizar.
   c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

      SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

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.

Antes de empezar

- 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 Core 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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 base de datos, debe utilizar el complemento de SnapCenter adecuado para la base de datos (por ejemplo, Complemento de SnapCenter para Microsoft SQL Server o Complemento de SnapCenter para Microsoft Exchange Server).

UI 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 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 snapshot.

   Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la 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. 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.

   b. En la sección Configure schedules for selected policies, haga clic en en la columna Configure Schedules de la política para la cual 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 **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"

6. 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. 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

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 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**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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
```

   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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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 base de datos, debe utilizar el complemento de SnapCenter adecuado para la base de datos (por ejemplo, Complemento de SnapCenter para Microsoft SQL Server o Complemento de SnapCenter para Microsoft Exchange Server).

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 seleccionado 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`.

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. 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.

  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.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

- El sitio de réplica está activo.
- El sitio de réplica está inactivo.
- No se restableció la relación de reflejo o almacén secundario.

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 **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una

programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

- Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.
- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.

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.

7. Si desea eliminar un clon, selecciónelo en la tabla y haga clic en para eliminar el clon.

Ejemplo que muestra backups y clones en el almacenamiento principal

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 Snapshot. Se recomienda utilizar este cmdlet cuando el total de las Snapshot que se muestran en la topología Manage Copies no corresponde al valor de retención de Snapshot del 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*. Alternativamente, 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.

   Este ejemplo borra el número de backups para backups secundarios sin snapshots:

```
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.

Antes de empezar

- 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.

Acerca de esta tarea

- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el

archivo SMCoreServiceHost.exe.Config del host del plugin.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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. 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.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

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.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, 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.

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

- Puede cancelar una operación de restauración en cola desde la página **Monitor** o desde el panel **actividad**.
- 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**. 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. 2. Seleccione la operación. 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.

Antes de empezar

- 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.

Acerca de esta tarea

- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el

archivo SMCoreServiceHost.exe.Config del host del plugin.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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 **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. 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.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

7. Revise el resumen y, a continuación, haga clic en **Finalizar**.
8. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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*. Alternativamente, 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

- Puede cancelar una operación de clonación en cola desde la página **Monitor** o desde el panel **actividad**.
- 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**. 2. Seleccione la operación y haga clic en **Cancelar trabajo**.

Del…	Acción
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. 2. Seleccione la operación. 3. En la página **Detalles del trabajo**, haz 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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"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.

El complemento para Exchange es compatible con la sincronización activa de SnapMirror (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), lo que permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo del sitio; de este modo, las aplicaciones pueden recuperarse tras fallos de forma transparente usando una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.

Es compatible con el modo asimétrico, de conmutación por error o no doble de SnapMirror Active Sync. Esto se refiere a la solución en la que la ruta optimizada es solo desde el nodo propietario de LUN del lado primario. Todas las operaciones de I/O que aparezcan en las rutas del clúster secundario reciben el servicio de proxy al clúster primario. La replicación síncrona es unidireccional, en la dirección del almacenamiento primario al secundario.

- 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
- Compatible con Exchange Server virtualizados en LUN de RDM cuando se pone en marcha el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter.

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 complemento SnapCenter para 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.

El soporte de aprovisionamiento y protección de datos de SnapCenter está disponible en Windows Server. Para obtener la información más reciente sobre las versiones compatibles, consulte la "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 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. 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 de ONTAP requeridos para el plugin de Exchange

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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo

- lun
- lun create
- lun create
- lun create
- eliminación de lun
- igroup de lun añadido
- crear lun igroup
- lun igroup eliminado
- cambio de nombre de lun igroup
- 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
- modificación de snapshot de volumen: snaplock: tiempo de caducidad
- 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
- 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 8.3.0 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.

SnapCenter realiza las actualizaciones de SnapMirror y SnapVault después de completar la operación de instantánea. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter . Si está utilizando la sincronización activa de SnapMirror , utilice las programaciones predeterminadas de SnapMirror o SnapVault tanto para la sincronización activa de SnapMirror como para las relaciones asincrónicas.

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 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. Una vez completado un backup completo, Exchange Server acorta los registros de transacciones que ya están confirmados en la base de datos. 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. No se realiza un backup de los registros de transacciones acortados.
Backup de registros	Realiza un backup de todos los registros de transacciones. 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 Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos

de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la 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

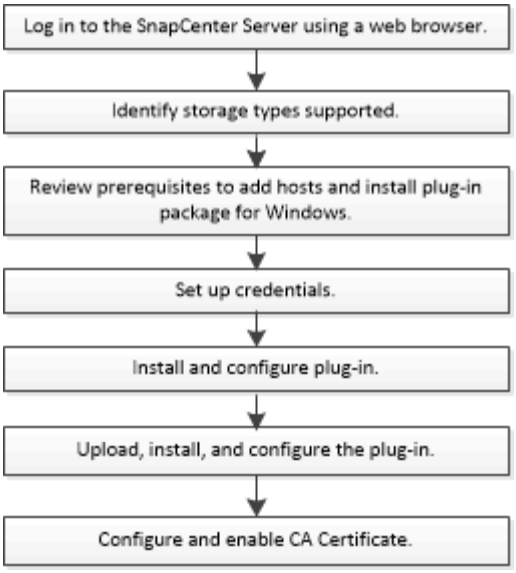
En una operación de restauración a un momento específico, las bases de datos se restauran únicamente a un punto específico. Esta operación se ejecuta en las siguientes situaciones:

- 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 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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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

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 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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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.
Nombre de usuario	Introduzca el nombre de usuario utilizado para autenticación. • 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` • 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`
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 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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 Add Host para añadir 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.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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 2016 o posterior para Microsoft Exchange Server".

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 un nodo de Exchange forma parte de un DAG, no puede añadir solo un nodo al servidor SnapCenter.
- 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.

A partir de SnapCenter 4.6, SCE admite multi-tenancy y puede añadir un host con los siguientes métodos:

Añadir una operación de host	4.5 y anteriores	4.6 y posterior
Agregar DAG sin IP en dominio cruzado o diferente	No admitido	Compatible
Agregue múltiples DAG IP con nombres únicos que residen en el mismo dominio o en varios dominios	Compatible	Compatible
Agregue múltiples DAG IP o sin IP que tengan los mismos nombres de host y/o nombre de base de datos en el dominio cruzado	No admitido	Compatible
Agregue múltiples DAG sin IP/IP con el mismo nombre y dominio cruzado	No admitido	Compatible
Agregue varios hosts independientes con el mismo nombre y entre dominios	No admitido	Compatible

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. Para obtener más información, consulte "Cómo registrar manualmente el proveedor de hardware VSS de Data ONTAP".

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, realice lo siguiente:

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione **Windows** como tipo de host. 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. 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.

Para este campo…	Realice lo siguiente…
Nombre de host	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 nombre de dominio completamente cualificado (FQDN). Una dirección IP es compatible para los hosts de dominio que no son de confianza solo si se resuelve en el FQDN. Si va a añadir un host mediante SnapCenter y forma parte de un subdominio, debe proporcionar el FQDN. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • DAG de Exchange Para un DAG de Exchange, puede: ◦ Añada un DAG proporcionando el nombre DAG, la dirección IP del DAG, el nombre de nodo o la dirección IP del nodo. ◦ Añada el clúster DAG sin IP mediante la dirección IP o el FQDN de uno de los nodos del clúster DAG. ◦ Añada el DAG IP sin que resida en el mismo dominio o en un dominio diferente. También puede agregar múltiples DAG IP/IP menos con el mismo nombre pero dominios diferentes. Para un host independiente o un DAG de Exchange (entre dominios o mismo dominio), se recomienda proporcionar un FQDN o la dirección IP del host o DAG.

Para este campo…	Realice lo siguiente…
Credenciales	Seleccione el nombre de la credencial que ha creado o cree las credenciales nuevas. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte los detalles de cómo crear una credencial. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. 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. 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. 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 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. Proporcione el nombre de GMSA con el siguiente formato: *Domainname\accountName$*. 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.

8. Supervise el progreso de la instalación.

Configure el puerto personalizado para la comunicación de NET TCP

De forma predeterminada, a partir de la versión SnapCenter 6,0, el plugin SnapCenter para Windows utiliza el puerto 909 para la comunicación de NET TCP. Si el puerto 909 está en uso, puede configurar otro puerto para la comunicación NET TCP.

Pasos

1. Modifique el valor de la clave *NetTCPPort* ubicada en *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config* al número de puerto requerido.
   `<add key="NetTCPPort" value="new_port_number" />`
2. Modifique el valor de la clave *NetTCPPort* ubicada en *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config* al número de puerto requerido.
   `<add key="NetTCPPort" value="new_port_number" />`
3. Anule el registro del servicio *Data ONTAP VSS Hardware Provider* ejecutando el siguiente comando:
   `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

Compruebe que el servicio no se muestra en la lista de servicios de *services.msc*.

4. Registre el servicio *Data ONTAP VSS Hardware Provider* ejecutando el siguiente comando:
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

   Compruebe si el servicio se muestra ahora en la lista de servicios de *services.msc*.

5. Reinicie el servicio *Plug-in para Windows*.

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.

Antes de empezar

- 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*. Alternativamente, 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.

3. 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.

Antes de empezar

- 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 el plugin.

   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.

   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: *Setup.exe /DEBUGLOG"C:\PathToLog\setupexe.log*

Variable	Valor
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.

6. 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*.
7. 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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$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.

Antes de empezar

- 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*. Alternativamente, 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.

Antes de empezar

- 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 su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM 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.

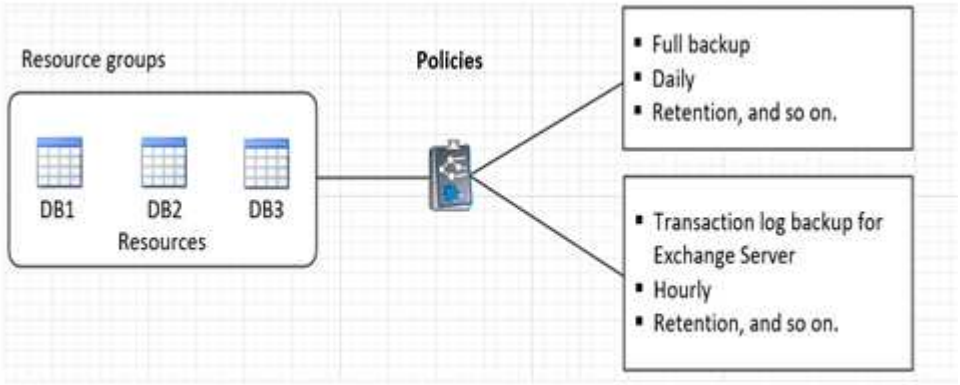
  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

  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

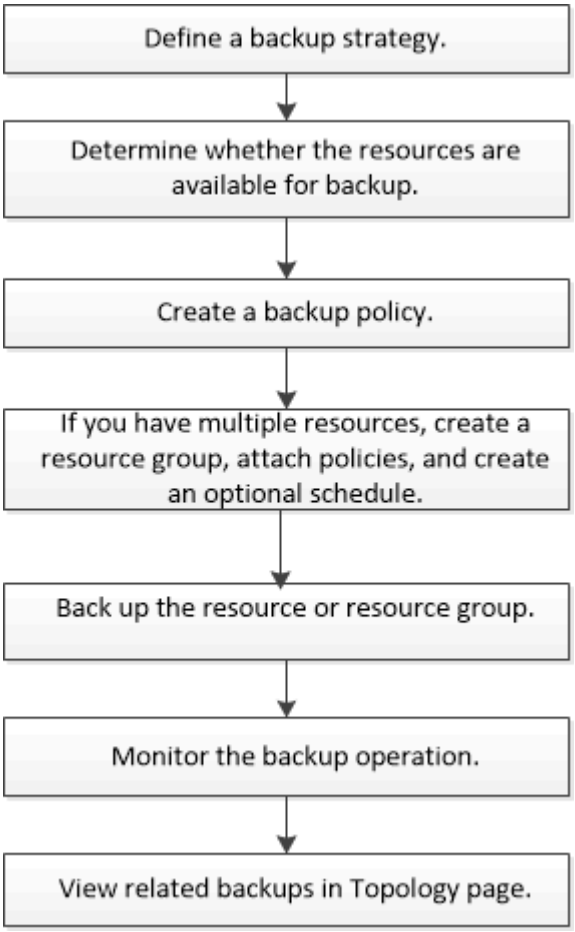
Flujo de trabajo de backup

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.

Antes de empezar

- 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**.

   Todas las bases de datos y los DAG se muestran con sus nombres de DAG o host en formato FQDN, por lo que es posible distinguir entre varias bases de datos.

   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.

   > Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

   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.

Antes de empezar

- 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 snapshots 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.

- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "Límites de objetos para la sincronización activa de SnapMirror".

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.
- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

  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. Cuando se configuran las políticas de retención secundarias, se tiene en cuenta que cuando las bases de datos y los registros que están en volúmenes diferentes, cada backup puede tener tres Snapshot y cuando las bases de datos y los registros están en el mismo volumen, cada backup puede tener dos Snapshot.

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.

    Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.

  Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las snapshots de SnapLock heredarán el tiempo de caducidad de SnapLock Vault. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 sus detalles.
5. En la página Backup Type and Replication, 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**. 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. 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**. 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**. Se realiza un backup de todos los registros de transacciones en el sistema de archivos activo y no hay truncamiento de registros. 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.
Realizar un backup de todos los archivos de la base de datos y los registros de transacciones sin acortarlos	Seleccione **copia de seguridad**. 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. 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. 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. 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.

a. Seleccione la etiqueta de política.

Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

b. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

Para este campo…	Realice lo siguiente…
Actualice SnapMirror después de crear una instantánea local	Seleccione esta opción para mantener copias de SnapMirror de conjuntos de backups en otro volumen (SnapMirror). Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Esta opción debe estar habilitada para la sincronización activa de SnapMirror. La política solo se puede usar si se configura la sincronización activa de SnapMirror para volúmenes de Exchange ONTAP. SnapCenter no permite esto. Debe activar la opción “Mirror”. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Consulte "Consulte los backups de Exchange en la página Topology".
Actualizar SnapVault después de crear una instantánea local	Seleccione esta opción para realizar una replicación de backup de disco a disco.
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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

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. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva 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. 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. 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. 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. **Mejores prácticas:** Es mejor que la configuración sea igual a la configuración de Total Snapshots (copias de seguridad completas) en la sección Configuración de retención de copia de seguridad completa. 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. Se conservan los backups de registros por la cantidad de días de backups completos.

Si desea…	Realice lo siguiente…
Período de bloqueo de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y seleccione Días, Meses o Años. El período de retención de SnapLock debe ser inferior a 100 años.

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…
Conserve únicamente una cantidad específica de snapshots	Si desea especificar el número de copias de seguridad completas que se deben conservar, seleccione la opción **Total de copias de Snapshot para mantener** y especifique el número de instantáneas (copias de seguridad completas) que se deben retener. 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 el número de días para conservar Snapshots (copias de seguridad completas).
Período de bloqueo de instantánea primaria	Seleccione **Periodo de bloqueo de copia de instantánea primaria** y seleccione Días, Meses o Años. El período de retención de SnapLock debe ser inferior a 100 años.
Período de bloqueo de instantánea secundaria	Seleccione **Periodo de bloqueo de copia de instantánea secundaria** y seleccione Días, Meses o Años.

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 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.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

8. 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.

Acerca de esta tarea

- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admite la adición de bases de datos nuevas sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de bases de datos nuevas a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

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 los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba el nombre del grupo de recursos. 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: Introduzca un nombre y un formato de Snapshot personalizados. Por ejemplo, *customtext_resourcegroup_policy_hostname* o *resourcegroup_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la 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 FQDN del host. Este FQDN solo indica que la base de datos está activa en ese host específico y que puede no realizar 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.

   b. Escriba el nombre del recurso en el cuadro de texto de búsqueda o desplácese para ubicar un recurso.

c. 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 Snapshot. Si hay más de 30 bases de datos en un grupo de recursos, se crea una segunda 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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

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.

Antes de empezar

- 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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.

UI de SnapCenter

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 terceros.

   > 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, 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.

   - 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. Si desea especificar un nombre de instantánea personalizado, en la página Recursos, active la casilla de comprobación **Use custom name format for Snapshot copy** y, a continuación, introduzca el formato del nombre personalizado que desee usar para el nombre de instantánea.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

4. 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 .

   > 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 Configure Schedules correspondiente a la política para la cual 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.

6. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de la base de datos.

7. Haga clic en **copia de seguridad ahora**.
8. 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**.
9. 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*

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/
```

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_Lo
g_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

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_Lo
g_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".

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.

Antes de empezar

- 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**.

   Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en * **y, luego, 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.

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.

Del…	Acción
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. 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 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.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

- El sitio de réplica está activo.
- El sitio de réplica está inactivo.
- No se restableció la relación de reflejo o almacén secundario.

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.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

   - Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.Después de la conmutación al nodo de respaldo.
   - Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.
5. 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.

6. 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.

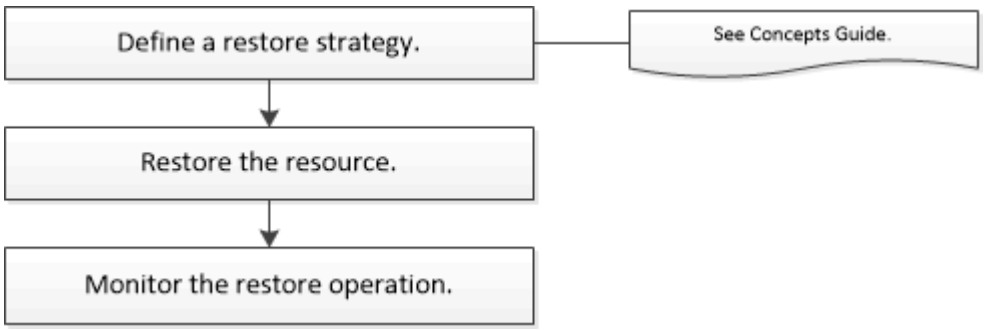
Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre. La eliminación de snapshots se gestiona mediante la configuración de retención de ONTAP.

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.

Para usar la funcionalidad de restauración por completo, se debe actualizar tanto SnapCenter Server como el plugin de SnapCenter para base de datos de Exchange a 4.6.

- 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.

Antes de empezar

- 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 snapshots 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.
- LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.

UI de SnapCenter

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. 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.

Opción	Descripción
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.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

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.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. 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.

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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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 Snapshots desde el almacenamiento principal hasta un almacenamiento secundario.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.

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**.

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.

Antes de empezar

Debe haber creado un backup de la base de datos que desea realimentar.

+ Para evitar la demora entre nodos, puede 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 Resources, seleccione la opción correspondiente en la lista View:

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 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.

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

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

- Puede cancelar una operación de restauración en cola desde la página **Monitor** o desde el panel **actividad**.
- 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**. 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. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**.

Proteger IBM DB2

Complemento de SnapCenter para IBM DB2

Información general sobre el plugin de SnapCenter para IBM DB2

El plugin de SnapCenter para bases de datos de IBM DB2 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 IBM DB2. El plugin para bases de datos de IBM DB2 automatiza el backup, la restauración y la clonado de bases de datos de IBM DB2 en el entorno de SnapCenter.

- SnapCenter 6,0 es compatible con IBM DB2 10,5 y versiones posteriores.
- SnapCenter 6.0.1 es compatible con IBM DB2 9,7.x y versiones posteriores. Asimismo, a partir de SnapCenter 6,0.1, se admite IBM DB2 en AIX.

SnapCenter admite configuraciones DB2 de instancia única y de varias instancias. Es posible utilizar el plugin para base de datos de IBM DB2 en entornos Linux y Windows. En entornos Windows, se admitirá DB2 como recurso manual.

El entorno pureScale DB2 y los sistemas de varios nodos (DPF) DB2 no son compatibles.

Cuando se instala el plugin para bases de datos de IBM DB2, 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.

El complemento SnapCenter para DB2 es compatible con NFS y SAN en distribuciones de almacenamiento de archivos de ONTAP y Azure NetApp.

Se admite la distribución de almacenamiento virtual VMDK, VVol y RDM.

Tareas que pueden llevarse a cabo con el plugin de SnapCenter para IBM DB2

Cuando el plugin para base de datos IBM DB2 está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar bases de datos IBM DB2 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 IBM DB2

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para base de datos IBM DB2, 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 instantánea NetApp no disruptiva**

  SnapCenter utiliza la tecnología de copias Snapshot de NetApp con el plugin para bases de datos IBM DB2 para realizar backups de recursos.

Usar el plugin para IBM DB2 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 Snapshot del grupo de coherencia (CG) 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 Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear snapshots con comandos externos
- Compatibilidad con LVM de Linux en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el plugin de SnapCenter para IBM DB2

SnapCenter es compatible con una amplia gama de tipos de almacenamiento tanto en máquinas físicas como máquinas virtuales (VM). Antes de instalar el plugin de SnapCenter para IBM DB2, debe comprobar la compatibilidad del tipo de

almacenamiento.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • 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. 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. • LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creado • Volúmenes NFS conectados directamente con el Guest VM • Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP requeridos para el plugin de IBM DB2

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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - lun
  - lun create

- lun create
- lun create
- eliminación de lun
- igroup de lun añadido
- crear lun igroup
- lun igroup eliminado
- cambio de nombre de lun igroup
- 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
- modificación de snapshot de volumen: snaplock: tiempo de caducidad
- 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
- 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 8.3.0 y versiones posteriores
  - interfaz de red
  - se muestra la interfaz de red
  - vserver

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para IBM DB2

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.

SnapCenter realiza las actualizaciones a SnapMirror y SnapVault después de que finaliza la operación de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.

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 IBM DB2

Definir una estrategia de backup para IBM DB2

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 Snapshot consistentes con las aplicaciones de la base de datos.
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 snapshots en el sistema de almacenamiento de origen y el destino de SnapMirror.
7. 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 e instancias de IBM DB2 en el host Linux gestionado por SnapCenter. Después de instalar el plugin de SnapCenter para IBM DB2, las bases de datos IBM DB2 de todas las instancias de ese host Linux se detectan automáticamente y se muestran en la página Resources.

Tipo de backups admitido

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite el tipo de backup basado en copias de Snapshot para las bases de datos IBM DB2.

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 IBM DB2.

Cómo utiliza el plugin de SnapCenter para IBM DB2 las snapshots de grupos de consistencia

Es posible usar el plugin para crear copias Snapshot de grupos de coherencia 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 coherencia es un conjunto de snapshots 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 snapshot de grupos consistentes. La sincronización WAFL mejora el rendimiento de una snapshot de grupo de coherencia.

Cómo hace SnapCenter para gestionar el mantenimiento de backups de datos

SnapCenter gestiona el mantenimiento de los backups de datos en los niveles de

sistema de almacenamiento y sistema de archivos.

Las snapshots en el almacenamiento primario y secundario y sus entradas correspondientes en el catálogo IBM DB2 se eliminan de acuerdo con la configuración de retención.

Consideraciones para determinar programaciones de backup para IBM DB2

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 IBM DB2

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 el plugin para bases de datos IBM DB2

Es posible usar la convención de nomenclatura de Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la Snapshot.

Estrategia de restauración y recuperación para IBM DB2

Defina una estrategia de restauración y recuperación para recursos de IBM DB2

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar una base de datos.

Sólo se admite la recuperación manual de la base de datos.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos IBM DB2 agregados manualmente
2. Determinar las estrategias de restauración compatibles con las bases de datos de IBM DB2 detectadas automáticamente

Tipos de estrategias de restauración compatibles con los recursos de IBM DB2 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 IBM DB2 agregados manualmente.

No se pueden recuperar recursos de IBM DB2 añadidos manualmente.

Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, las copias de Snapshot tomadas después de la copia de Snapshot seleccionada para restaurar en 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.

Tipo de estrategia de restauración compatible con el IBM DB2 detectado automáticamente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter.

La restauración de recursos completa es la estrategia de restauración compatible con las bases de datos IBM DB2 detectadas automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para el IBM DB2 autodetectado

El plugin de SnapCenter para IBM DB2 es compatible con SnapRestore de archivo único, y los tipos de restauración por conexión y copia para bases de datos IBM DB2 detectadas automáticamente.

Single File SnapRestore se realiza en entornos NFS en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- Cuando la copia de seguridad seleccionada se realiza desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **completar recurso**

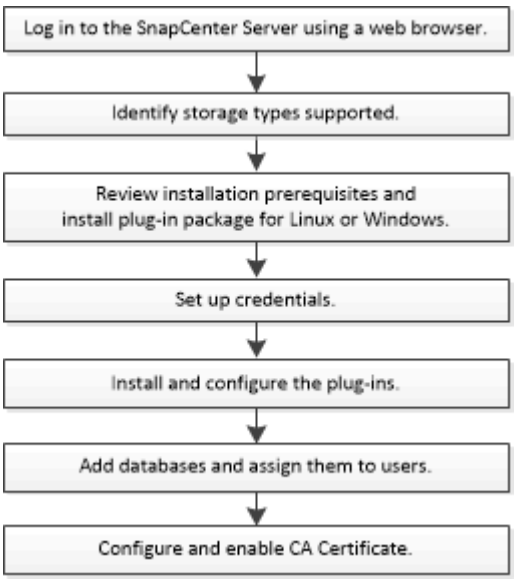
Single File SnapRestore se realiza en entornos SAN en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- Cuando se selecciona la copia de seguridad de una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Complete Resource**

Prepare la instalación del plugin de SnapCenter para IBM DB2

Flujo de trabajo de instalación del plugin de SnapCenter para IBM DB2

Tendrá que instalar y configurar el plugin de SnapCenter para IBM DB2 si desea proteger las bases de datos de IBM DB2.



Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. El plugin de SnapCenter para IBM DB2 es compatible con entornos Windows, Linux y AIX.

- Debe haber instalado Java 11 en el host.

  IBM Java no es compatible con el host Windows y Linux.

- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows 'LocalSystem', que es el comportamiento predeterminado cuando el plugin para IBM DB2 se instala como administrador de dominio.
- 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 implementará de forma predeterminada con el plugin IBM DB2 en hosts de Windows.
- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host IBM DB2.

Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Al instalar el plugin para IBM DB2 en un host de 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 11 en el host de Windows.

  "Descargar JAVA para Windows"

Hosts Linux y AIX

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

  "Descargar JAVA para Linux"

  "Descargar JAVA para AIX"

- Para bases de datos IBM DB2 que se ejecutan en un host Linux, cuando se instala el plugin para IBM DB2, el plugin de SnapCenter para UNIX se instala automáticamente.
- Debe tener **bash** como shell por defecto para la instalación del plug-in.

Comandos suplementarios

Para ejecutar un comando complementario en el plugin de SnapCenter para IBM DB2, debe incluirlo en el archivo *allowed_commands.config*.

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementarios en el host del plugin, abra el archivo *allowed_commands.config* en un editor. Escriba cada comando en una línea diferente y los comandos no distinguen mayúsculas de minúsculas. Asegúrese de especificar el nombre de ruta completamente cualificado y escribirlo entre comillas si contiene

espacios.

Por ejemplo:

comando: mount

comando: umount

Comando: «C:\Program Files\NetApp\SnapCreator commands\sdcli.exe»

comando: myscript.bat

Si el archivo *allowed_commands.config* no está presente, los comandos o la ejecución del script se bloquearán y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

Si el comando o script no está presente en *allowed_commands.config*, el comando o la ejecución del script se bloqueará y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

No debe utilizar una entrada comodín (*) para permitir todos los comandos.

Configure privilegios sudo para usuarios que no son raíz para el host Linux

SnapCenter permite que un usuario no raíz instale el paquete de plugins de SnapCenter para Linux e inicie el proceso del plugin. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- Para el usuario que no es root, asegúrese de que el nombre del usuario que no es root y del grupo del usuario debe ser el mismo.
- 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/*LINUX_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 HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.

- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- 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 HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

AIX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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 Para obtener la información más reciente sobre las versiones compatibles, consulte la "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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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 • SUSE Linux Enterprise Server (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Elemento	Requisitos
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 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	Java 11 Oracle Java y OpenJDK 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.

Configure credenciales para el plugin de SnapCenter para IBM DB2

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 Settings, haga clic en **Credential**.
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.
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • 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* • 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* 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.

Para este campo…	Realice lo siguiente…
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. Aplicable únicamente a usuarios Linux.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, se recomienda asignar el mantenimiento de credenciales a un usuario o un grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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 IBM DB2

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.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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 2016 o posterior para IBM DB2"

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: • Windows • Linux El plugin para IBM DB2 está instalado en el host de cliente IBM DB2, y este host puede estar en un sistema Windows o Linux.

Para este campo…	Realice lo siguiente…
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.
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. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado. 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.

   Mientras utiliza la API DE REST para instalar el plugin para DB2, debe pasar la versión como 3,0. Por ejemplo, DB2:3,0

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. 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	El plugin para IBM DB2 está instalado en el host de cliente IBM DB2, y este host puede estar en un sistema Windows o Linux. • 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. • Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta.
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. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. 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, . La versión de NET, la ubicación (para plugins de Windows) y Java 11 (tanto para plugins de Windows como 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.

9. Supervise el progreso de la instalación.
   - Para el plugin de Windows, los registros de instalación y actualización se encuentran en: *C:\Windows\SnapCenter plugin\Install*<JOBID>\
   - Para el plugin de Linux, los registros de instalación se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log y los registros de actualización se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log

Después de terminar

Si desea actualizar a SnapCenter 6,0 o posterior, el plugin basado en PERL para DB2 existente se desinstala del servidor de plugins remoto.

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.

Antes de empezar

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*. Alternativamente, 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.

4. Introduzca sus credenciales para la instalación remota.

Instale el plugin de SnapCenter para IBM DB2 en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para base de datos IBM DB2 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 IBM DB2 en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

Antes de empezar

- Debe instalar el plugin para base de datos IBM DB2 en cada host Linux en el que resida el cliente IBM DB2.
- El host Linux en el que se instala el plugin de SnapCenter para base de datos IBM DB2 debe cumplir con los requisitos dependientes de software, base de datos y sistema operativo.

  El "Herramienta de matriz de interoperabilidad (IMT)" Contiene la información más reciente sobre las configuraciones compatibles.

- El plugin de SnapCenter para base de datos IBM DB2 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.

Acerca de esta tarea

Si no se mencionan los parámetros, SnapCenter se instala con los valores predeterminados.

Pasos

1. Copie el archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar el plugin para IBM DB2.

   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. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y, a continuación, añada el parámetro PLUGINS_ENABLED = DB2:3,0.
5. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervise el estado de instalación del plugin para IBM DB2

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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configure el certificado de CA para el servicio de plugins de SnapCenter IBM DB2 en el host Linux

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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 del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento: /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 para complementar el almacén de confianza.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento /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 del almacén de claves del complemento predeterminado es el valor de la clave 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 firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para complementos

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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 de SnapCenter IBM DB2 en el host Windows

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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*.

4. Reinicie el servicio después de cambiar la contraseña.

   La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 para complementar el almacén de confianza.

   Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 del almacén de claves del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos 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 de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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.

Antes de empezar

- 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*. Alternativamente, 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 el plugin de SnapCenter para IBM DB2

Antes de utilizar el plugin de SnapCenter para IBM DB2, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y llevar a cabo 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 11 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.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger IBM DB2

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 de IBM DB2 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.

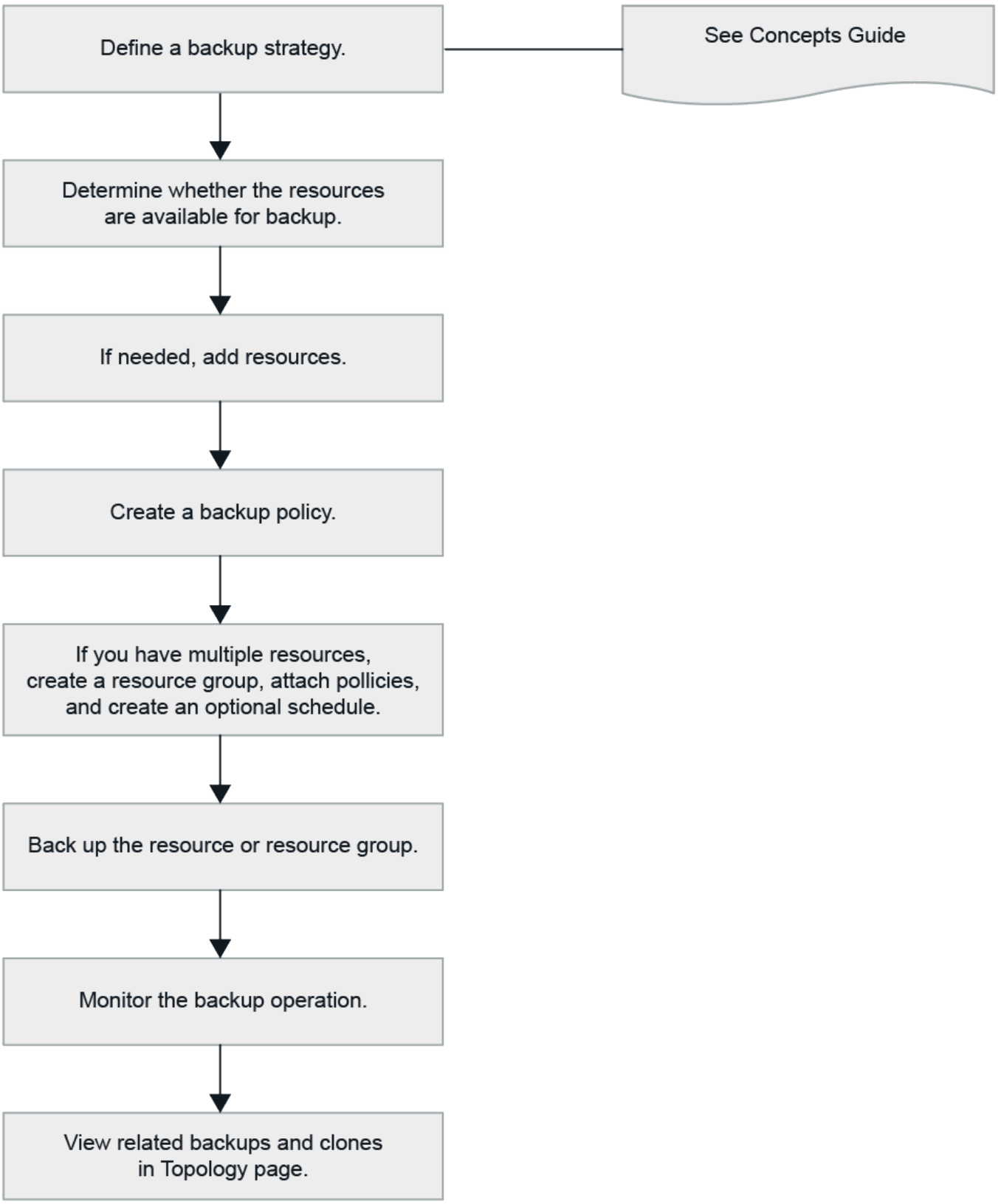
Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos 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 IBM DB2

Realice un backup de los recursos de IBM DB2

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. "Guía de referencia de cmdlets de SnapCenter Software".

Detectar las bases de datos automáticamente

Los recursos son bases de datos de IBM DB2 en el host Linux gestionados por SnapCenter. Es posible añadir los recursos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos IBM DB2 disponibles.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts y configurar las conexiones del sistema de almacenamiento.
- El plugin de SnapCenter para IBM DB2 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, se detectan automáticamente todas las bases de datos en ese host Linux y se muestran en la página Resources.
- Solo se detectan automáticamente las bases de datos.

Los recursos de detección automática no se pueden modificar ni eliminar.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin para IBM DB2 de la lista.
2. En la página Resources, seleccione el tipo de recurso en la lista View.
3. (Opcional) Haga clic en y 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.

Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

Añada recursos manualmente al host del plugin

El host Windows no admite la detección automática. Debe añadir manualmente las instancias y los recursos de la base de datos de DB2.

Antes de empezar

- Debe haber completado tareas como instalar SnapCenter Server, añadir hosts y configurar conexiones del sistema de almacenamiento.

Acerca de esta tarea

La detección manual no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin de SnapCenter para IBM DB2 en la lista desplegable.
2. En la página Recursos, haga clic en **Agregar recurso de IBM DB2**.
3. En la página Provide Resource Details, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre	Especifique el nombre de la base de datos.
Nombre de host	Introduzca el nombre de host.
Tipo	Seleccione la base de datos o la instancia.
Instancia	Especifique el nombre de la instancia, que es el elemento principal de la base de datos.
Credenciales	Seleccione las credenciales o agregue información para la credencial. Esto es opcional.

4. En la página Provide Storage Footprint, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees y, 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. Opcional: En la página Resource Settings, en el caso de los recursos del host de Windows, introduzca pares de clave-valor personalizados para el plugin de IBM DB2
6. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Las bases de datos se muestran junto con información como el nombre del host, las políticas y los 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 agregar las bases de datos, es posible modificar los detalles de la base de datos IBM DB2.

Crear políticas de backup para IBM DB2

Antes de usar SnapCenter para realizar un backup de recursos de IBM DB2, 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.

Antes de empezar

- Debe tener definida una estrategia de backup.

  Para obtener detalles, consulte la información sobre cómo definir una estrategia de protección de datos para las bases de datos IBM DB2.

- 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 snapshots 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.

Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de instantáneas, se evita la eliminación de las instantáneas hasta que caduque el período de retención. Esto podría provocar que se retenga un número mayor de instantáneas que el recuento especificado en la política.
  - Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 sus detalles.
5. En la página Policy type, realice lo siguiente:
   a. Seleccione el tipo de almacenamiento.
   b. 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.

6. En la página Snapshot and Replication, realice las siguientes acciones.

   a. Especifique la frecuencia de programación 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.

   a. En la sección Snapshot settings, realice las siguientes acciones:

Si desea…	Realice lo siguiente…
Conserve un cierto número de instantáneas	Seleccione **Copias para mantener** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de copias de Snapshot supera el número especificado, las copias de Snapshot se eliminan empezando por las más antiguas.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y especifique días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

      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 snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva snapshot en el destino.

   b. Especifique la etiqueta de la política.

      Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

7. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

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). Esta opción debe estar habilitada para la sincronización activa 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).
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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

8. 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.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. 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.
Use 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 snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la snapshot.

4. En la página Resources, 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 Application Settings, realice 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…
Espere tiempo a que finalice la operación de snapshot de grupo de consistencia	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que se complete la operación de instantánea. 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 PRE y POST para las operaciones de inactividad, instantánea y desactivación. 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.
RETENCIÓN_LOG_ARCHIVO	número_de_días	Especifica la cantidad de días que se conservan los registros de archivo. 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. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.16151855 1942 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. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

Los pares de clave-valor personalizados son compatibles con los sistemas de plugins de Linux IBM DB2 y no son compatibles con la base de datos IBM DB2 registrada como un plugin de Windows centralizado.

c. Haga clic en la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

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**.
SnapCenter para crear una snapshot a nivel del almacenamiento	Seleccione **SnapCenter sin coherencia del sistema de archivos**.
Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot.	Seleccione **Otro** y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

7. 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 + .

Las políticas figuran en la sección Configure schedules for selected policies.

b. En la columna Configure Schedules, haga clic en + en la política 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.

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. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

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

Cree grupos de recursos y habilite la protección secundaria para recursos IBM DB2 en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:

a. Seleccione el tipo de política de replicación.

No se admite la política de replicación síncrona.

b. Especifique el sufijo del grupo de consistencia que desea utilizar.

c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para IBM DB2

Es necesario 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 IBM DB2.

Antes de empezar

- 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. Haga clic en **SnapCenterPS** para iniciar PowerShell Core.
2. Cree una nueva conexión con el sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

   ```
   PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
   -OntapStorage 'scsnfssvm' -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' -Type Linux
   -AuthenticationType PasswordBased -Credential db2hostuser
   -EnableSudoPrevileges:$true
   ```

4. Agregue el host de comunicación IBM DB2 al servidor SnapCenter.

   Para Linux:

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

Para Windows:

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. Instale el paquete y el plugin de SnapCenter para IBM DB2 en el host.

   Para Linux:

   ```
   PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
   DB2
   ```

   Para Windows:

   ```
   PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
   DB2,SCW
   ```

6. Defina la ruta de acceso a SQLLIB.

   Para Windows, el plugin DB2 utilizará la ruta predeterminada para la carpeta SQLLIB: “C:\Program Files\IBM\SQLLIB\BIN”

   Si desea anular la ruta predeterminada, utilice el comando siguiente.

   ```
   PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
   -PluginCode DB2 -configSettings
   @{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
   ```

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

Realizar un backup de las bases de datos de DB2

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.

Antes de empezar

- 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 la operación de backup basado en copias de Snapshot, asegúrese de que todas las bases de datos de tenant sean válidas y estén activas.
- Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y la reanudación de la copia, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin con las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

UI de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Seleccione , y, a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede seleccionar cerrar el panel de filtros.
3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.
5. En la página Application Settings, realice lo siguiente:

   - Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales:

     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

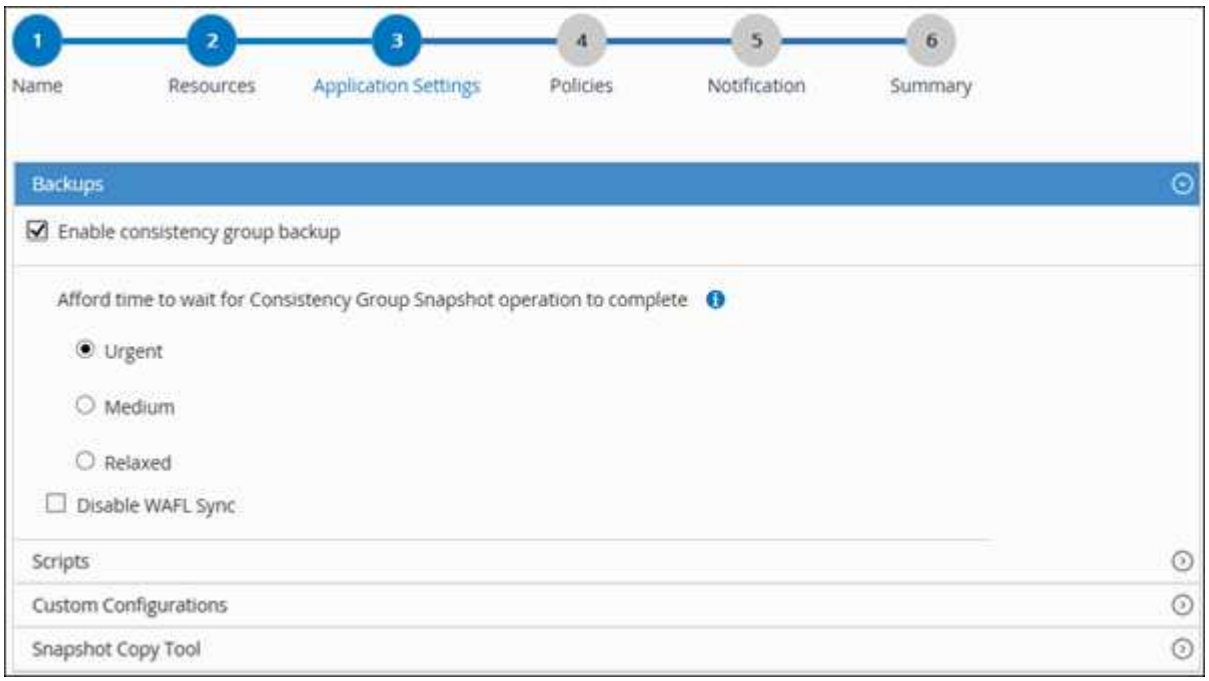
Para este campo…	**Realice lo siguiente…**
Permitir que se complete la operación de "Snapshot de grupo de consistencia"	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que finalice la operación de instantánea. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.

   - Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.

     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.
   - Seleccione la flecha **Configuraciones personalizadas**y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
   - Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	**Realice lo siguiente…**
SnapCenter cree una snapshot a 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**.
Para escribir el comando para crear una snapshot	Seleccione **Otro** y luego ingrese el comando para crear una instantánea.



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. Seleccione + En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

      policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

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. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

8. Revisa el resumen y luego selecciona **Finalizar**.

   Se muestra la página de topología de los recursos.

9. Seleccione **Back up Now**.
10. En la página Backup, 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. Seleccione **copia de seguridad**.
11. 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"

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.

   ```
   PS C:\> Open-SmConnection
   ```

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada recursos manuales mediante el cmdlet Add-SmResources.

   Este ejemplo muestra cómo agregar una instancia de IBM DB2:

   ```
   PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
   -ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
   (@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
   geSystem"="scsnfssvm"}) -MountPoints "D:\"
   ```

   Para la base de datos DB2:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
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_Db2_Resources' -Policy db2_policy1
   ```

   Este ejemplo realiza un backup de una instancia de DB2:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
   db2_policy
   ```

   Este ejemplo realiza un backup de una base de datos DB2:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDB";"PluginName"="DB2"
   } -Policy db2_policy
   ```

6. Supervise el estado de la tarea (running, completed o failed) mediante el cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-SmJobSummaryReport -JobId 467

SmJobId            : 467
JobCreatedDateTime :
JobStartDateTime   : 27-Jun-24 01:40:09
JobEndDateTime     : 27-Jun-24 01:41:15
JobDuration        : 00:01:06.7013330
JobName            : Backup of Resource Group
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
'snapshot-based-db2'
JobDescription     :
Status             : Completed
IsScheduled        : False
JobError           :
JobType            : Backup
PolicyName         : db2_policy
JobResultData      :
```

7. 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 467

BackedUpObjects           : {WINCIR}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 84
SmJobId                   : 467
StartDateTime             : 27-Jun-24 01:40:09
EndDateTime               : 27-Jun-24 01:41:15
Duration                  : 00:01:06.7013330
CreatedDateTime           : 27-Jun-24 18:39:45
Status                    : Completed
ProtectionGroupName       : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId       : 23
PolicyName                : db2_policy
SmPolicyId                : 13
BackupName                : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DB2
PluginDisplayName         : IBM DB2
JobTypeId                 :
JobHost                   : HOSTFQDN
```

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

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.

Antes de empezar

- 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 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, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos escribiendo su nombre en el cuadro de búsqueda o seleccionando y, luego, seleccionar la etiqueta. A continuación, puede seleccionar cerrar el panel de filtros.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **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. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Supervisar las operaciones de copia de seguridad de IBM DB2

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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 las bases de datos IBM DB2 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Cancelar las operaciones de copia de seguridad de IBM DB2

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. 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 de IBM DB2 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, 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.

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 del número de copias de seguridad y clones disponibles en el almacenamiento principal y secundario.

   La sección **Summary Card** muestra el número total de copias de Snapshot y clones.

   Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Después de la copia de seguridad a petición, haciendo clic en el botón **Actualizar** actualiza los detalles de la copia de seguridad o clonación.

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 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.

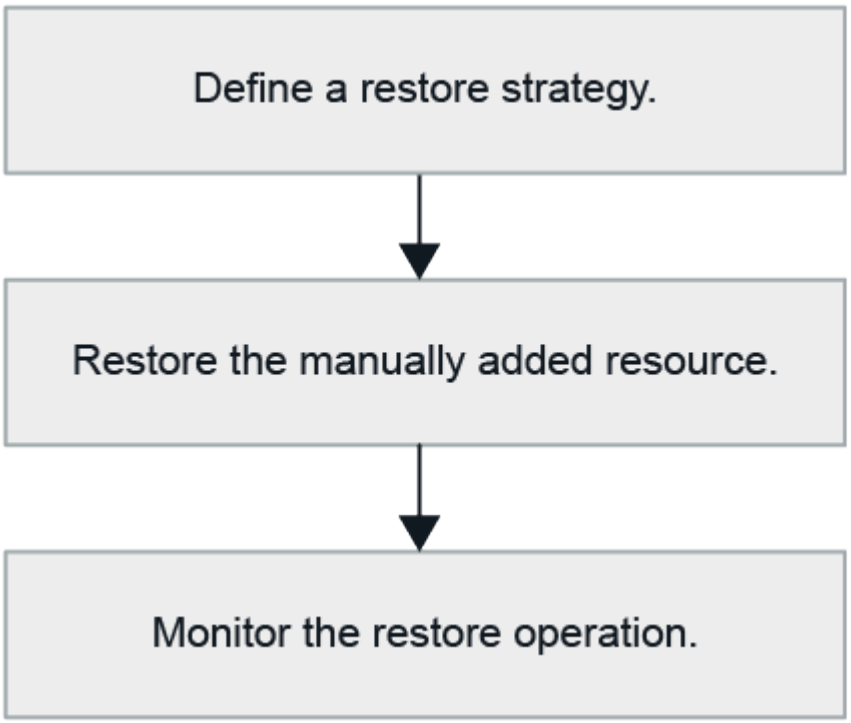
7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
8. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Restaurar IBM DB2

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 un backup de recursos añadido manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje,

debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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.

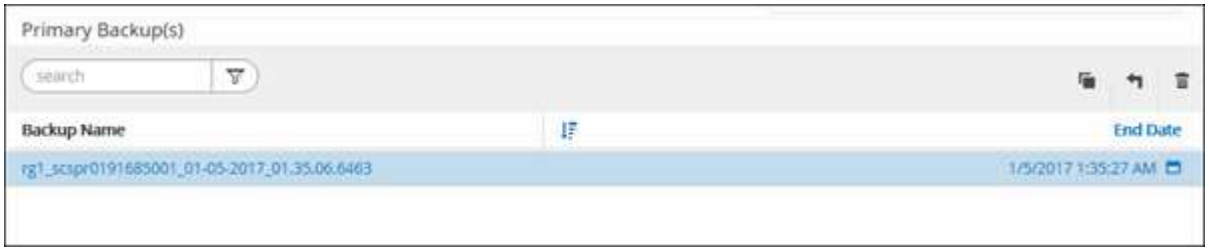
   > Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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**.

   a. Si selecciona **Recurso completo**, se restauran todos los volúmenes de datos configurados de la base de datos IBM DB2.

      Si el recurso contiene volúmenes o qtrees, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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.

      Puede seleccionar varios LUN.

      > Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.

7. 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.
8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la

restauración que se ejecutarán después de realizar un trabajo de restauración.

9. 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 la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

La recuperación sólo es posible si el estado Rollforward está pendiente de base de datos. Este estado es aplicable a las bases de datos DB2 con archive log activado.

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.

```
PS C:\> Open-SmConnection
```

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 -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\Library

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM  Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

   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. Puede restaurar los datos del backup mediante el cmdlet Restore-SmBackup.

> AppObjectId es «Host\Plugin\UID», donde UID = <instance_name> es para un recurso de instancia de DB2 detectado manualmente y UID = <instance_name>\<databse_name> es para un recurso de base de datos IBM DB2. Puede obtener el ResourceID a partir del cmdlet Get-smResources.

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode DB2
```

Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento primario:

```
Restore-SmBackup -PluginCode DB2 -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento secundario:

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

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

Restaurar y recuperar un backup de base de datos detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para los recursos detectados automáticamente, se admite la restauración con SFSR.
- No se admite la recuperación automática.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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, filtre los recursos de la lista desplegable **View** 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.

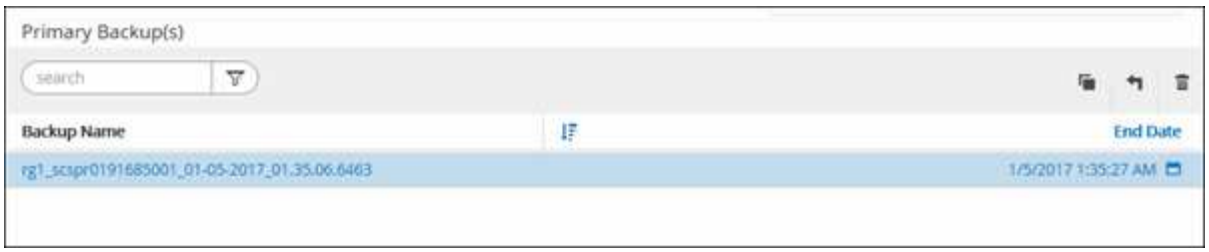
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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 IBM DB2.
7. 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 se requieren para los recursos detectados automáticamente.

8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no se necesitan para los recursos detectados automáticamente.

9. 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 la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

La recuperación sólo es posible si el estado Rollforward está pendiente de base de datos. Este estado es

aplicable a las bases de datos DB2 con archive log activado.

Supervisar las operaciones de restauración de IBM DB2

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.

Clonar backups de recursos de IBM DB2

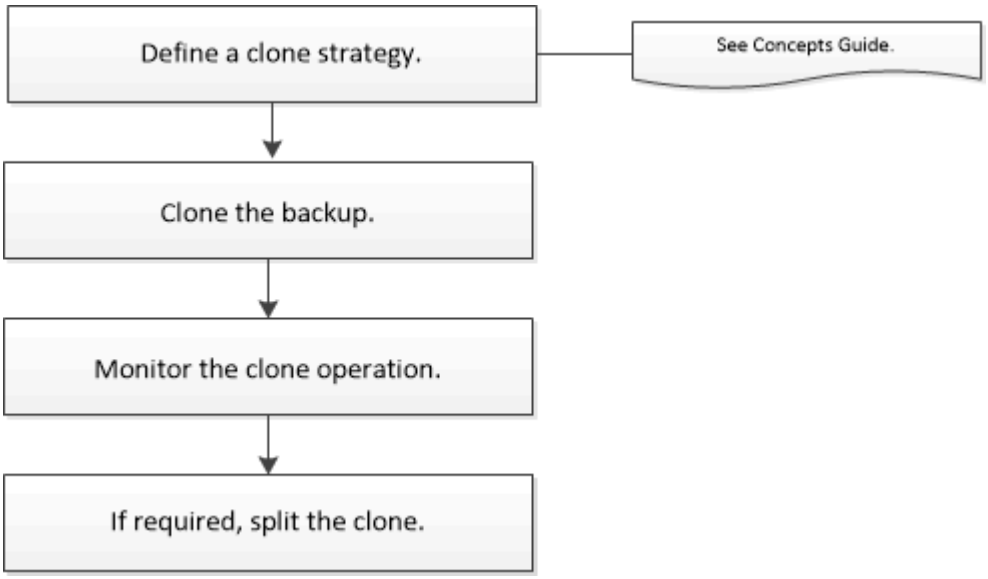
Flujo de trabajo de clonado

El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

Acerca de esta tarea

- Puede clonar en el servidor IBM DB2 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.

Después de terminar

Después de clonar los recursos DB2 detectados automáticamente, el recurso clonado se marca como recurso manual. Haga clic en **Refrescar recursos** para recuperar el recurso DB2 clonado. Cuando se elimina el clon, también se limpian el almacenamiento y el host.

Si no se actualizan los recursos después de la operación de clonado e intentan eliminar el clon, no se limpian el almacenamiento y el host. Debe eliminar las entradas manualmente en fstab.

Clonar un backup de IBM DB2

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario.

Antes de empezar

- 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).
- Al crear un clon para DB2 en un host alternativo, debe crear una estructura de directorio n-1 para la ruta de montaje del clon igual que la ruta de montaje original en el otro host. La ruta de acceso de montaje

debe tener el permiso de ejecución *755*.

- Para los comandos previos o posteriores a la clonado, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para obtener más información sobre las operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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 Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el servidor	Elija el host donde se debe crear el clon.
Instancia de Clonación de Destino	Introduzca el ID de instancia de clon objetivo DB2 para clonar a partir de los backups existentes. Esto solo es aplicable a los recursos del tipo de almacenamiento ANF.
Nombre de clon de destino	Introduzca el nombre del clon. Esto es aplicable solo para el recurso de base de datos DB2.
Dirección IP de exportación NFS	Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados. Esto solo se aplica al recurso de tipo de almacenamiento NFS.
Pool de capacidad máx. Rendimiento (MiB/s)	Introduzca el rendimiento máximo de un pool de capacidad.

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 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.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

Después de clonar los recursos DB2 detectados automáticamente, el recurso clonado se marca como recurso manual. Haga clic en **Refrescar recursos** para recuperar el recurso DB2 clonado. Cuando se elimina el clon, también se limpian el almacenamiento y el host.

Si no se actualizan los recursos después de la operación de clonado e intentan eliminar el clon, no se limpian el almacenamiento y el host. Debe eliminar las entradas manualmente en fstab.

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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervisar las operaciones de clonación de IBM DB2

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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

Elimine o divida clones de base de datos IBM DB2 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 primario de la página Resources.

   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 en para dividir los

clones.

7. Haga clic en **Aceptar**.

Proteger PostgreSQL

Complemento de SnapCenter para PostgreSQL

Información general sobre el plugin de SnapCenter para PostgreSQL

El plugin de SnapCenter para PostgreSQL es un componente en el lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de clústeres PostgreSQL. El clúster del plugin para PostgreSQL automatiza el backup, la restauración y la clonado de clústeres de PostgreSQL en el entorno de SnapCenter.

SnapCenter admite configuraciones PostgreSQL en un solo clúster y múltiples clústeres. Es posible utilizar el plugin para clústeres de PostgreSQL en entornos Linux y Windows. En entornos Windows, PostgreSQL será soportado como recurso manual.

Cuando se instala el clúster del plugin para PostgreSQL, 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.

El complemento de SnapCenter para PostgreSQL es compatible con NFS y SAN en distribuciones de almacenamiento de archivos de ONTAP y Azure NetApp.

Se admite la distribución de almacenamiento virtual VMDK, VVol y RDM.

Tareas que pueden llevarse a cabo con el plugin de SnapCenter para PostgreSQL

Cuando se instala el clúster del plugin para PostgreSQL en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar clústeres de PostgreSQL y sus recursos. También es posible ejecutar tareas complementarias a estas operaciones.

- Añadir clústeres.
- 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 PostgreSQL

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para clúster PostgreSQL, 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 instantánea NetApp no disruptiva**

  SnapCenter utiliza la tecnología Snapshot de NetApp con el clúster del plugin para PostgreSQL para realizar backups de recursos.

Usar el plugin para PostgreSQL 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 Snapshot del grupo de coherencia (CG) 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 Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear snapshots con comandos externos
- Compatibilidad con LVM de Linux en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el plugin de SnapCenter para PostgreSQL

SnapCenter es compatible con una amplia gama de tipos de almacenamiento tanto en máquinas físicas como máquinas virtuales (VM). Antes de instalar el plugin de SnapCenter para PostgreSQL, debe comprobar la compatibilidad de su tipo de almacenamiento.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • 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. 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. • LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS • Volúmenes NFS conectados directamente con el Guest VM • Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP requeridos para el plugin de PostgreSQL

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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - lun
  - lun create
  - lun create
  - lun create

- eliminación de lun
- igroup de lun añadido
- crear lun igroup
- lun igroup eliminado
- cambio de nombre de lun igroup
- 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
    - modificación de snapshot de volumen: snaplock: tiempo de caducidad
    - 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
    - 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 8.3.0 y versiones posteriores
    - interfaz de red

- se muestra la interfaz de red
- vserver

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para PostgreSQL

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.

SnapCenter realiza las actualizaciones a SnapMirror y SnapVault después de que finaliza la operación de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.

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 PostgreSQL

Defina una estrategia de backup para PostgreSQL

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 copias de Snapshot consistentes con las aplicaciones del clúster.
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 snapshots en el sistema de almacenamiento de origen y el destino de SnapMirror.
7. 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 clústeres e instancias de PostgreSQL en el host Linux que son administrados por SnapCenter. Después de instalar el plugin de SnapCenter para PostgreSQL, los clústeres PostgreSQL de todas las instancias de ese host Linux se detectan automáticamente y se muestran en la página Resources.

Tipo de backups admitido

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite el tipo de backup basado en copias de Snapshot para clústeres de PostgreSQL.

Backup basado en copia de Snapshot

Los backups basados en copia de Snapshot aprovechan la tecnología de copia Snapshot de NetApp para crear copias en línea y de solo lectura de los volúmenes en los cuales residen los clústeres de PostgreSQL.

Cómo usa el plugin de SnapCenter para PostgreSQL las snapshots de grupos de consistencia

Es posible usar el plugin para crear copias Snapshot de grupos de coherencia 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 coherencia es un conjunto de snapshots 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 snapshot de grupos consistentes. La sincronización WAFL mejora el rendimiento de una snapshot de grupo de coherencia.

Cómo hace SnapCenter para gestionar el mantenimiento de backups de datos

SnapCenter gestiona el mantenimiento de los backups de datos en los niveles de sistema de almacenamiento y sistema de archivos.

Las instantáneas en el almacenamiento primario o secundario y sus entradas correspondientes en el catálogo

PostgreSQL se eliminan de acuerdo con la configuración de retención.

Consideraciones para determinar programaciones de backup para PostgreSQL

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 PostgreSQL

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 clústeres del plugin para PostgreSQL

Es posible usar la convención de nomenclatura de Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la Snapshot.

Estrategia de restauración y recuperación para PostgreSQL

Defina una estrategia de restauración y recuperación para recursos PostgreSQL

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar un clúster.

Solo se admite la recuperación manual del clúster.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos PostgreSQL añadidos manualmente
2. Determinar las estrategias de restauración compatibles con clústeres PostgreSQL detectados automáticamente
3. Decidir el tipo de operaciones de recuperación que se desea ejecutar.

Tipos de estrategias de restauración compatibles con los recursos PostgreSQL añadidos manualmente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter.

No se pueden recuperar recursos PostgreSQL añadidos manualmente.

Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, las copias de Snapshot tomadas después de la copia de Snapshot seleccionada para restaurar en 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.

NOTA: El plugin para PostgreSQL crea una etiqueta de copia de seguridad y un mapa de tablespace en la carpeta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ para ayudar a recuperar manualmente.

Tipo de estrategia de restauración compatible con PostgreSQL detectado automáticamente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter.

La restauración completa de recursos es la estrategia de restauración compatible con los clústeres de PostgreSQL detectados automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para PostgreSQL auto descubierta

El plugin de SnapCenter para PostgreSQL es compatible con SnapRestore de archivo único, y los tipos de restauración por conexión y copia para los clústeres de PostgreSQL detectados automáticamente.

Single File SnapRestore se realiza en entornos NFS en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- 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:

- Si solo se selecciona la opción **Complete Resource**
- Cuando se selecciona la copia de seguridad de una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Complete Resource**

Tipos de operaciones de recuperación compatibles con los clústeres PostgreSQL

SnapCenter permite ejecutar diferentes tipos de operaciones de recuperación para clústeres de PostgreSQL.

- Recupere el clúster hasta el estado más reciente
- Recupere el clúster hasta un momento específico

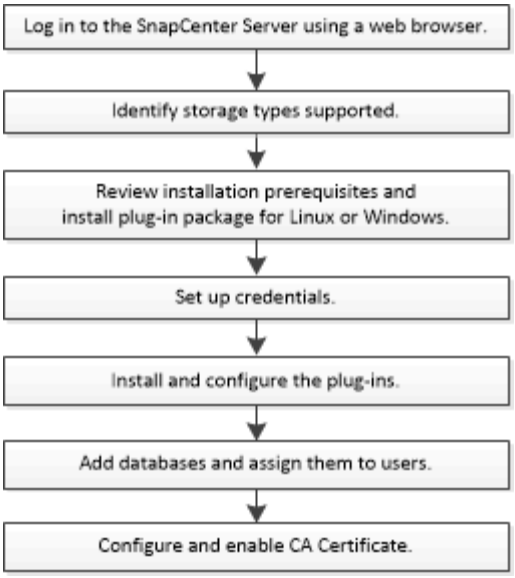
  Debe especificar la fecha y la hora de la recuperación.

SnapCenter también proporciona la opción No recovery para los clústeres PostgreSQL.

Prepare la instalación del plugin de SnapCenter para PostgreSQL

Flujo de trabajo de instalación del plugin de SnapCenter para PostgreSQL

Debe instalar y configurar el plugin de SnapCenter para PostgreSQL si desea proteger los clústeres de PostgreSQL.



Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para PostgreSQL

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. El complemento SnapCenter para PostgreSQL está disponible en entornos Windows y Linux.

- Debe haber instalado Java 11 en el host.

  IBM Java no es compatible con el host Windows y Linux.

- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows 'LocalSystem', que es el comportamiento predeterminado cuando el plugin para PostgreSQL se instala como administrador de dominio.
- 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 PostgreSQL en hosts de Windows.
- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host de PostgreSQL.

Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Al instalar el plugin para PostgreSQL en un host de 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 11 en el host de Windows.

  "Descargar JAVA para todos los sistemas operativos"

Hosts Linux

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

  "Descargar JAVA para todos los sistemas operativos"

- Para los clústeres PostgreSQL que se ejecutan en un host Linux, cuando se instala el plugin para PostgreSQL, el plugin de SnapCenter para UNIX se instala de forma automática.
- Debe tener **bash** como shell por defecto para la instalación del plug-in.

Comandos suplementarios

Para ejecutar un comando complementario en el plugin de SnapCenter para PostgreSQL, debe incluirlo en el archivo *allowed_commands.config*.

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementarios en el host del plugin, abra el archivo *allowed_commands.config* en un editor. Escriba cada comando en una línea diferente y los comandos no distinguen mayúsculas de minúsculas. Asegúrese de especificar el nombre de ruta completamente cualificado y escribirlo entre comillas si contiene espacios.

Por ejemplo:

Comando: Comando de montaje: Comando umount: C:\Program Files\NetApp\SnapCreator commands\sdcli.exe. myscript.bat

Si el archivo *allowed_commands.config* no está presente, los comandos o la ejecución del script se bloquearán y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

Si el comando o script no está presente en *allowed_commands.config*, el comando o la ejecución del script se bloqueará y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

No debe utilizar una entrada comodín (*) para permitir todos los comandos.

Configure privilegios sudo para usuarios que no son raíz para el host Linux

SnapCenter permite que un usuario no raíz instale el paquete de plugins de SnapCenter para Linux e inicie el proceso del plugin. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.

- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- Para el usuario que no es root, asegúrese de que el nombre del usuario que no es root y del grupo del usuario debe ser el mismo.
- 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/*LINUX_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 HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- _C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ si el servidor SnapCenter está instalado en el host de Windows.
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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

Elemento	Requisitos
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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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 • SUSE Linux Enterprise Server (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "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 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	Java 11 Oracle Java y OpenJDK 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.

Configure credenciales para el plugin de SnapCenter para PostgreSQL

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 clústeres o sistemas de archivos Windows.

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 Settings, haga clic en **Credential**.
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.
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • 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* • 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* 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.

Para este campo…	Realice lo siguiente…
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. Aplicable únicamente a usuarios Linux.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, se recomienda asignar el mantenimiento de credenciales a un usuario o un grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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 PostgreSQL

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 el host e instalar paquetes de plugins para un host individual.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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 administrada de grupo en Windows Server 2016 o posterior para PostgreSQL"

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: • Windows • Linux El plugin para PostgreSQL está instalado en el host de cliente PostgreSQL, y este host puede estar en un sistema Windows o Linux.

Para este campo…	Realice lo siguiente…
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.
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. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado. 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.

   Mientras utiliza la API de REST para instalar el plugin para PostgreSQL, debe pasar la versión como 3,0. Por ejemplo, PostgreSQL:3,0

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. 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	El plugin para PostgreSQL está instalado en el host de cliente PostgreSQL, y este host puede estar en un sistema Windows o Linux. • 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. • Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta.
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.
Añada todos los hosts del clúster	Seleccione esta casilla de comprobación para añadir todos los nodos del clúster.
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. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. 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.

9. Supervise el progreso de la instalación.
   - Para el plugin de Windows, los registros de instalación y actualización se encuentran en: *C:\Windows\SnapCenter plugin\Install*<JOBID>_
   - Para el plugin de Linux, los registros de instalación se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ y los registros de actualización se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

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.

Antes de empezar

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*. Alternativamente, 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.

4. Introduzca sus credenciales para la instalación remota.

Instale el plugin de SnapCenter para PostgreSQL en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para clúster PostgreSQL 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 clúster PostgreSQL en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos

(CLI).

Antes de empezar

- Debe instalar el clúster del plugin para PostgreSQL en cada host Linux en el que resida el cliente PostgreSQL.
- El host Linux en el que se instala el plugin de SnapCenter para PostgreSQL debe cumplir con los requisitos dependientes de software, clúster y sistema operativo.

  El "Herramienta de matriz de interoperabilidad (IMT)" Contiene la información más reciente sobre las configuraciones compatibles.

- El plugin de SnapCenter para el clúster PostgreSQL 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 archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar el plugin para PostgreSQL.

   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. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y, a continuación, añada el parámetro PLUGINS_ENABLED = PostgreSQL:3,0.
5. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervise el estado de instalación del plugin para PostgreSQL

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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configure el certificado de CA para el servicio de plugins PostgreSQL de SnapCenter en el host Linux

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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 del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento: /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 para complementar el almacén de confianza.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento /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 del almacén de claves del complemento predeterminado es el valor de la clave 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 firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para complementos

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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 PostgreSQL de SnapCenter en el host Windows

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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*.

4. Reinicie el servicio después de cambiar la contraseña.

   La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 para complementar el almacén de confianza.

   Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 del almacén de claves del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos 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 de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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.

Antes de empezar

- 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*. Alternativamente, 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 el plugin de SnapCenter para PostgreSQL

Antes de utilizar el plugin de SnapCenter para PostgreSQL, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y ejecutar 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 11 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.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger PostgreSQL

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 clústeres PostgreSQL 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.

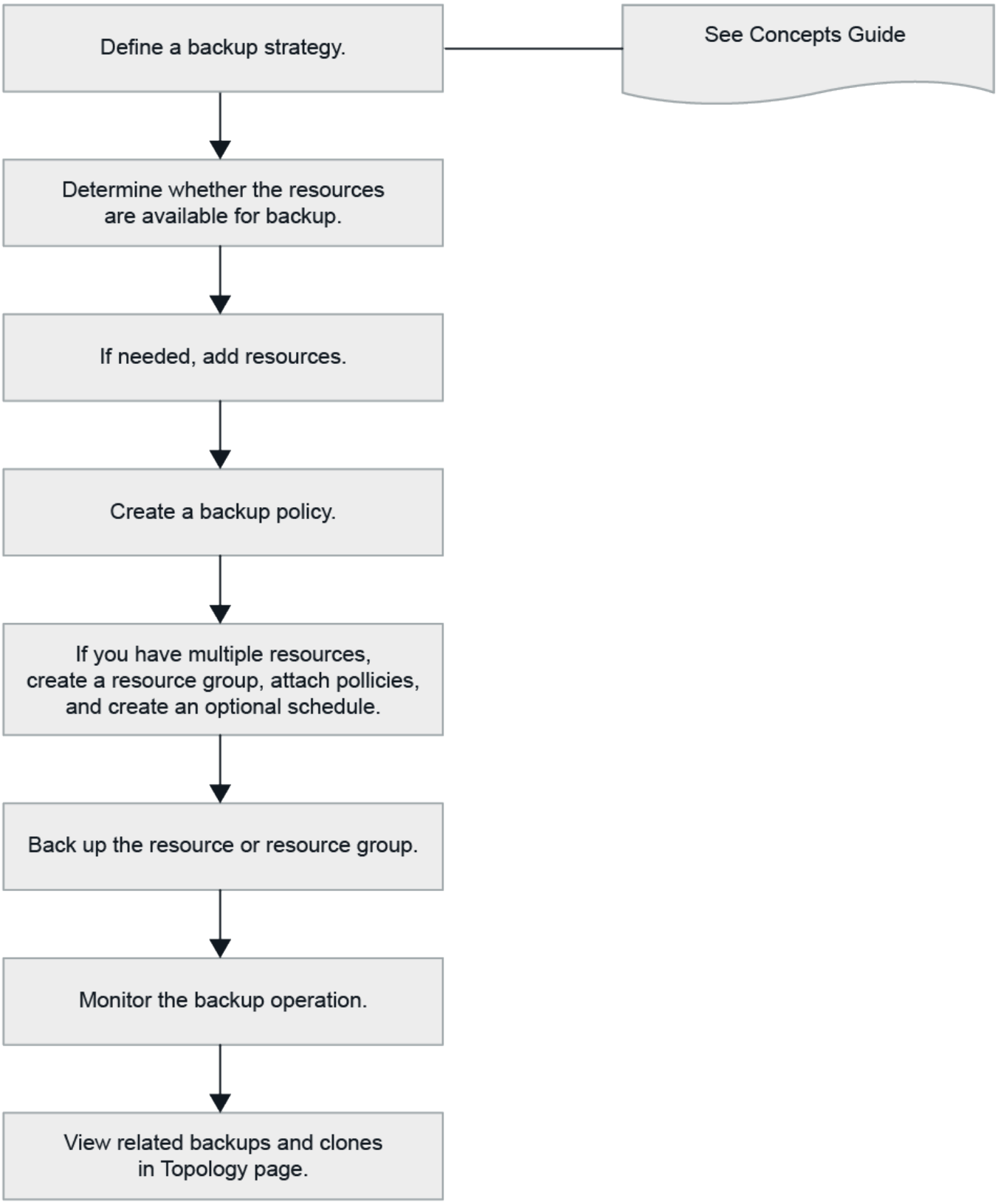
Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de todos los clústeres, por ejemplo, puede crear un grupo de recursos que incluya todos los clústeres 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.

Hacer backup de recursos de PostgreSQL

Hacer backup de recursos de PostgreSQL

Es posible crear un backup de un recurso (clúster) o un grupo de recursos. El flujo de trabajo de backup incluye planificar, identificar los clústeres para 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. 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".

Detecte los clústeres automáticamente

Los recursos son clústeres PostgreSQL en el host Linux que administra SnapCenter. Es posible añadir los recursos a grupos de recursos para realizar operaciones de protección de datos después de detectar los clústeres de PostgreSQL disponibles.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts y configurar las conexiones del sistema de almacenamiento.
- El plugin de SnapCenter para PostgreSQL no admite la detección automática de los recursos que residen en entornos virtuales de RDM/VMDK.

Acerca de esta tarea

- Después de instalar el plugin, se detectan automáticamente todos los clústeres en ese host Linux y se muestran en la página Resources.
- Solo los clústeres se detectan automáticamente.

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, a continuación, seleccione el plugin para PostgreSQL de la lista.
2. En la página Resources, seleccione el tipo de recurso en la lista View.
3. (Opcional) Haga clic en y 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 el clúster está en un almacenamiento de NetApp y no está protegido, se muestra Not protected en la columna Overall Status.
   - Si el clúster se encuentra en un sistema de almacenamiento de NetApp y está protegido, y si no hay operación de backup ejecutada, se muestra Backup 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.

Los recursos se deben actualizar si se cambia el nombre de los clústeres fuera de SnapCenter.

Añada recursos manualmente al host del plugin

El host Windows no admite la detección automática. Debe añadir manualmente los recursos del clúster de PostgreSQL.

Antes de empezar

- Debe haber completado tareas como instalar SnapCenter Server, añadir hosts y configurar conexiones del sistema de almacenamiento.

Acerca de esta tarea

La detección automática no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

Pasos

1. En el panel de navegación izquierdo, seleccione el plugin de SnapCenter para PostgreSQL en la lista desplegable y, a continuación, haga clic en * Recursos *.
2. En la página Recursos, haga clic en **Agregar recursos PostgreSQL**.
3. En la página Provide Resource Details, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre	Especifique el nombre del clúster.
Nombre de host	Introduzca el nombre de host.
Tipo	Seleccione el clúster.
Instancia	Especifique el nombre de la instancia, que es el elemento principal del clúster.
Credenciales	Seleccione las credenciales o agregue información para la credencial. Esto es opcional.

4. En la página Provide Storage Footprint, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees y, 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. Opcional: En la página Resource Settings, en el caso de los recursos del host de Windows, introduzca pares de clave-valor personalizados para el plugin de PostgreSQL
6. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Los clústeres se muestran junto con información, como el nombre del host, las políticas y los 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 terminar

- Después de añadir los clústeres, puede modificar los detalles del clúster PostgreSQL.
- Los recursos migrados (tablespace y clusters) de SnapCenter 5,0 se etiquetarán como tipo de cluster

PostgreSQL en SnapCenter 6,0.

- Cuando modifique los recursos agregados manualmente que se migran desde SnapCenter 5,0 o una versión anterior, haga lo siguiente en la página **Configuración de recursos** para pares de valores de clave personalizados:
  - Especifique el término “PUERTO” en el campo **Nombre**.
  - Especifique el número de puerto en el campo **Valor**.

Crear políticas de backup para PostgreSQL

Antes de usar SnapCenter para realizar un backup de recursos de PostgreSQL, debe crear una política de backup para el recurso o grupo de recursos que desee incluir en el backup. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups.

Antes de empezar

- Debe tener definida una estrategia de backup.

  Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para clústeres de PostgreSQL.

- 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 snapshots 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.

Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de instantáneas, se evita la eliminación de las instantáneas hasta que caduque el período de retención. Esto podría provocar que se retenga un número mayor de instantáneas que el recuento especificado en la política.
  - Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 sus detalles.
5. En la página Policy type, realice lo siguiente:
   a. Seleccione el tipo de almacenamiento.

b. 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.

6. En la página Backup and Replication, realice las siguientes acciones:

a. Especifique la frecuencia de programación 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.

a. En la sección Configuración de instantánea, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionado en la página **Tipo de copia de seguridad**:

Si desea…	Realice lo siguiente…
Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino. El valor máximo de retención es 1018. Las copias de seguridad fallarán si la retención se establece en un valor superior al que admite la versión de ONTAP .

Si desea…	Realice lo siguiente…
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y especifique días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

7. Seleccione una etiqueta de política.

Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

8. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

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). Si la relación en ONTAP es del tipo Reflejo y almacén y solo se selecciona esta opción, Snapshot creado en el origen no se transferirá al destino, pero figurará en el destino. Si esta copia 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. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Consulte "Consulte los backups y los clones relacionados con los recursos de PostgreSQL en la página Topology".

Para este campo…	Realice lo siguiente…
Actualizar SnapVault después de crear una copia Snapshot local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el almacén de SnapLock, consulte Confirmar instantáneas en WORM en un almacén destino Consulte "Consulte los backups y los clones relacionados con los recursos de PostgreSQL en la página Topology".
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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

9. 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.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad

de SnapLock.

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 los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. 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.
Use 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 snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la snapshot.

4. En la página Resources, 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.

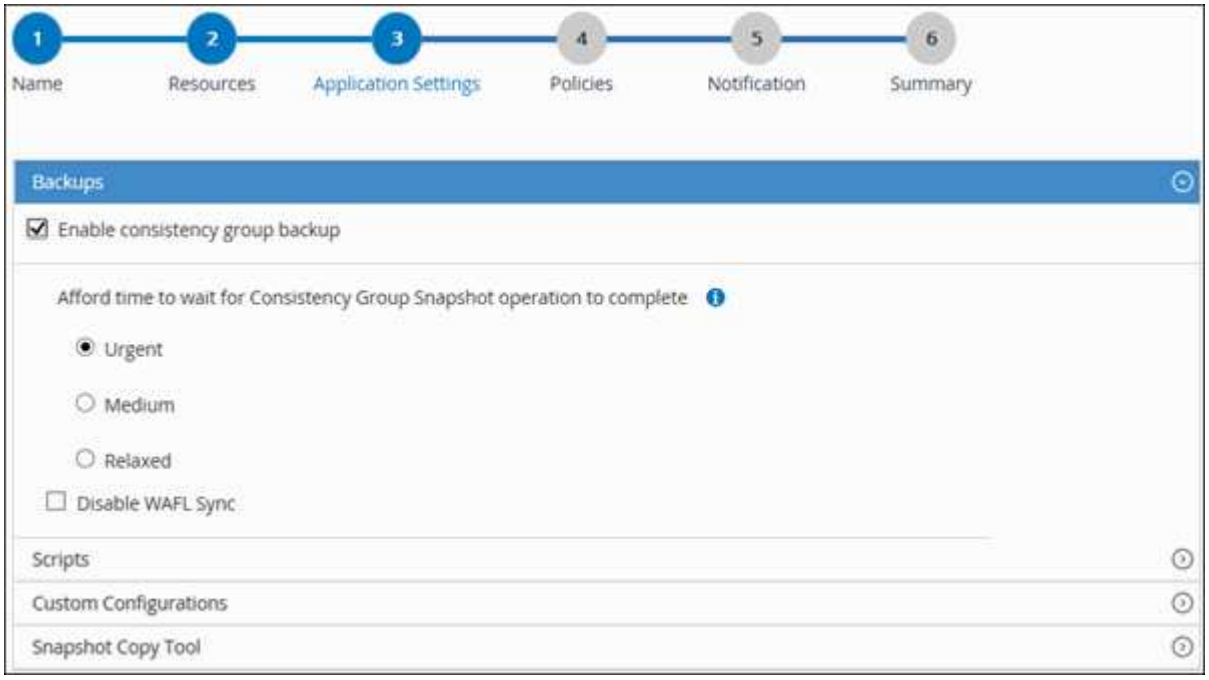
5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. En la página Application Settings, realice lo siguiente:

   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…
Espere tiempo a que finalice la operación de snapshot de grupo de consistencia	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que se complete la operación de instantánea. 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 PRE y POST para las operaciones de inactividad, instantánea y desactivación. 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. 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 extensión del archivo de registro de archivo. Por ejemplo, si el registro de archivo es log_backup_0_1.log, especifique .log como la extensión del archivo.
ARCO ARCHIVE_LOG_RECURSIVE_ SE	(S/N)	Permite la gestión de registros de ficheros en subdirectorios. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

Los pares clave-valor personalizados son compatibles con los sistemas de plugins de Linux PostgreSQL y no son compatibles con el clúster PostgreSQL registrado como un plugin centralizado de Windows.

c. Haga clic en la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

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**.
SnapCenter para crear una snapshot a nivel del almacenamiento	Seleccione **SnapCenter sin coherencia del sistema de archivos**.
Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot.	Seleccione **Otro** y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

7. 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 + .

      Las políticas figuran en la sección Configure schedules for selected policies.

   b. En la columna Configure Schedules, haga clic en + en la política 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.

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. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

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

Cree grupos de recursos y habilite la protección secundaria para recursos de PostgreSQL en sistemas R2 de ASA

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.

3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

      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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:
   a. Seleccione el tipo de política de replicación.

      No se admite la política de replicación síncrona.

   b. Especifique el sufijo del grupo de consistencia que desea utilizar.
   c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

      SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para PostgreSQL

Es necesario crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar cmdlets de PowerShell para realizar backup, restaurar o clonar clústeres PostgreSQL.

Antes de empezar

- 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 plugins de host en curso mientras se añade una conexión a sistemas de almacenamiento, porque la caché del host puede no estar actualizada y el estado de los clústeres puede mostrarse en la interfaz gráfica de usuario de SnapCenter con el formato «`Not available for backup`» o «`Not on NetApp storage`».

- 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 Core mediante el cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

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. Agregue el host de comunicación PostgreSQL al servidor SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode PostgreSQL
```

5. Instale el paquete y el plugin de SnapCenter para PostgreSQL en el host.

   Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL
```

   Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina la ruta de acceso a SQLLIB.

   Para Windows, el plugin PostgreSQL utilizará la ruta predeterminada para la carpeta SQLLIB: “C:\Program Files\IBM\SQLLIB\BIN”

   Si desea anular la ruta predeterminada, utilice el comando siguiente.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

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

Backup de PostgreSQL

Si un recurso aún no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

Antes de empezar

- 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 la operación de backup basado en copias de Snapshot, asegúrese de que todos los clústeres de inquilinos sean válidos y estén activos.
- Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y la reanudación de la copia, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin con las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

UI de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Seleccione * * y, a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede seleccionar cerrar el panel de filtros.
3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.
5. En la página Application Settings, realice lo siguiente:

   - Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales:

     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

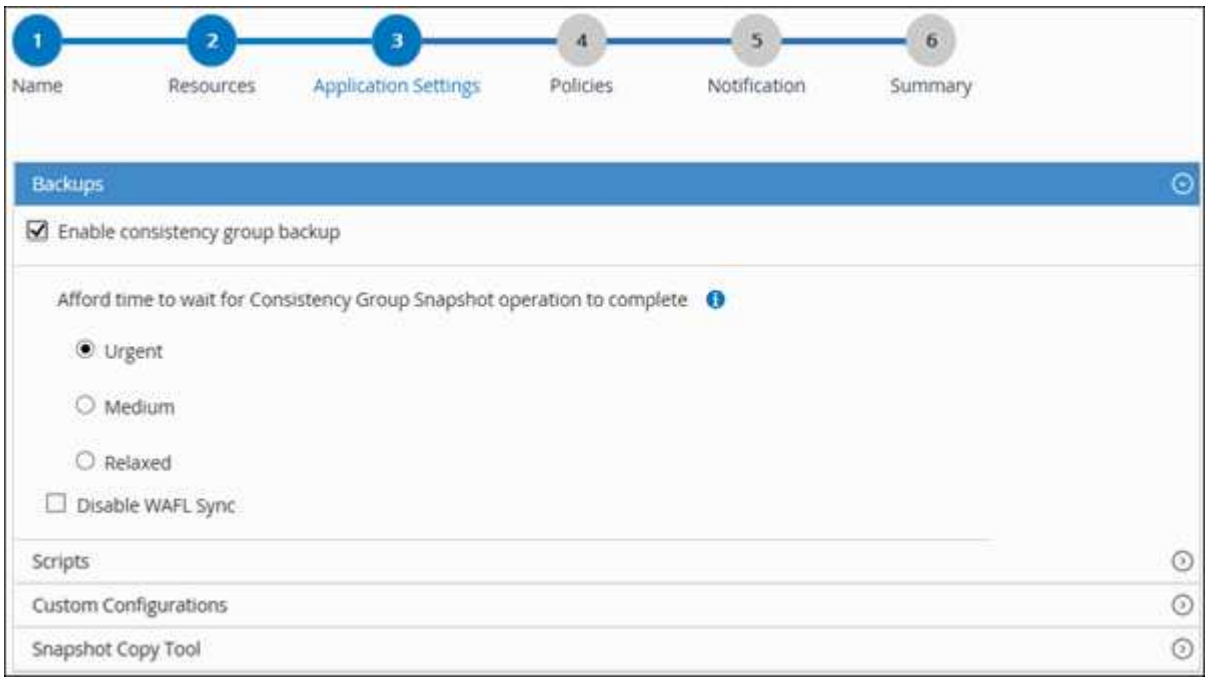
Para este campo…	**Realice lo siguiente…**
Permitir que se complete la operación de "Snapshot de grupo de consistencia"	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que finalice la operación de instantánea. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.

   - Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.

     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.
   - Seleccione la flecha **Configuraciones personalizadas**y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
   - Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	**Realice lo siguiente…**
SnapCenter cree una snapshot a 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**.
Para escribir el comando para crear una snapshot	Seleccione **Otro** y luego ingrese el comando para crear una instantánea.



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. Seleccione + en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

      policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

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. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

8. Revisa el resumen y luego selecciona **Finalizar**.

   Se muestra la página de topología de los recursos.

9. Seleccione **Back up Now**.
10. En la página Backup, 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. Seleccione **copia de seguridad**.
11. 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*

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.

   ```
   PS C:\> Open-SmConnection
   ```

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada recursos manuales mediante el cmdlet Add-SmResources.

   Este ejemplo muestra cómo agregar una instancia PostgreSQL:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
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_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Este ejemplo realiza un backup de un recurso protegido:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

6. Supervise el estado de la tarea (running, completed o failed) mediante el cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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 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, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos escribiendo su nombre en el cuadro de búsqueda o seleccionando y, luego, seleccionar la etiqueta. A continuación, puede seleccionar cerrar el panel de filtros.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **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. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Supervisar las operaciones de backup de PostgreSQL

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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 clústeres PostgreSQL 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Cancelar las operaciones de backup para PostgreSQL

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. 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 de PostgreSQL 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, 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.

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 del número de copias de seguridad y clones disponibles en el almacenamiento principal y secundario.

   La sección **Summary Card** muestra el número total de copias de Snapshot y clones.

   Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Después de la copia de seguridad a petición, haciendo clic en el botón **Actualizar** actualiza los detalles de la copia de seguridad o clonación.

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 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.

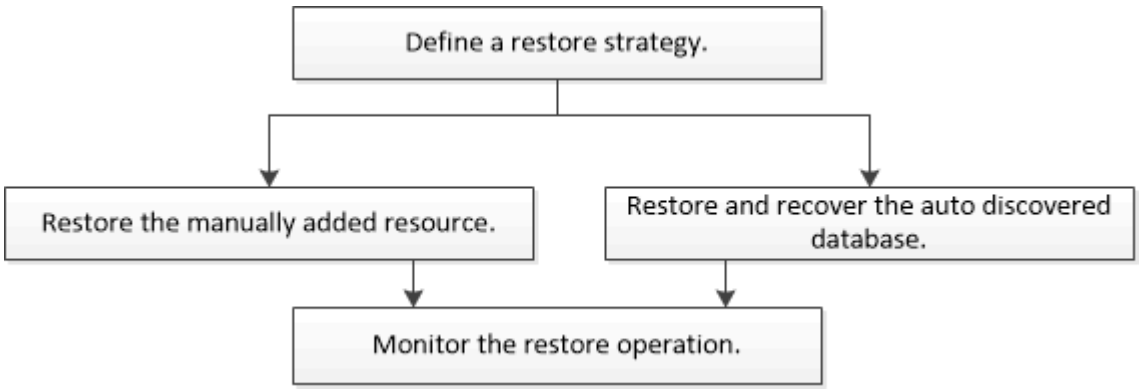
7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
8. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Restaurar PostgreSQL

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.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad

de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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.

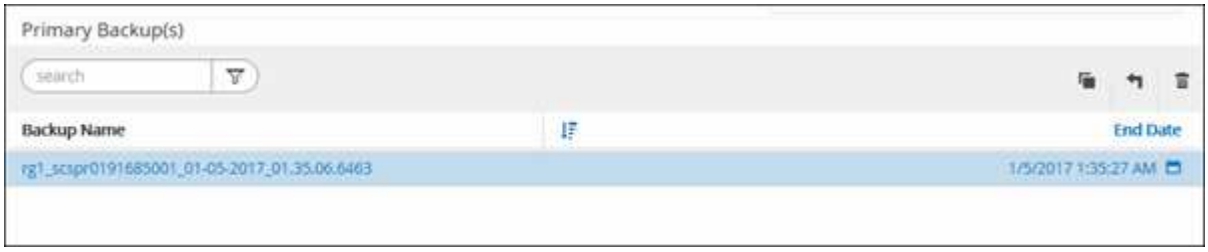
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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**.

   a. Si selecciona **Recurso completo**, se restauran todos los volúmenes de datos configurados del clúster PostgreSQL.

      Si el recurso contiene volúmenes o qtrees, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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.

      Puede seleccionar varios LUN.

      Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.

7. 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.

8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

9. 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 la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Restaure y recupere un backup de clúster detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Las copias de backup basadas de archivos no se pueden restaurar desde SnapCenter.
- Para los recursos detectados automáticamente, se admite la restauración con SFSR.
- No se admite la recuperación automática.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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, filtre los recursos de la lista desplegable **View** 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.

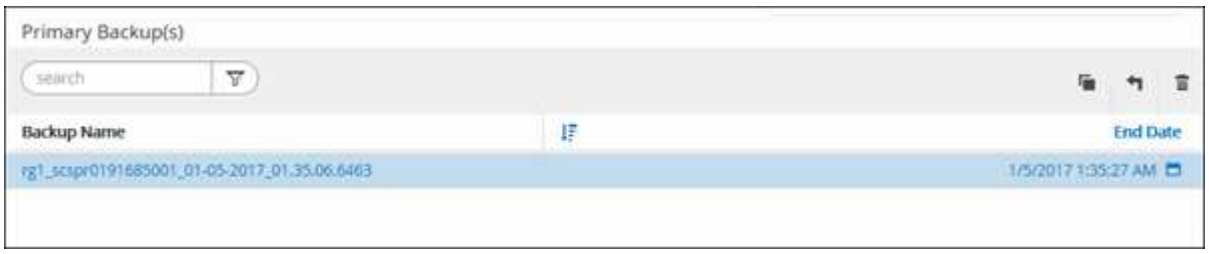
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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 del clúster PostgreSQL.

7. En la página Restore Scope, 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.
Desea recuperar al punto en el tiempo especificado	Seleccione **Recover to point in time**. a. Introduzca la fecha y la hora. Introduzca la fecha y la hora. Por ejemplo, el host PostgreSQL Linux se encuentra en Sunnyvale, CA y el usuario en Raleigh, NC está recuperando los registros en SnapCenter. Si el usuario desea realizar una recuperación a 5 a.m . Sunnyvale, CA, entonces el usuario debe establecer la zona horaria del navegador en la zona horaria del host de PostgreSQL Linux, que es GMT-07:00 y especificar la fecha y la hora como 5:00 a.m.
No desea recuperar	Seleccione **sin recuperación**.

No se pueden recuperar recursos PostgreSQL añadidos manualmente.

El plugin de SnapCenter para PostgreSQL crea una etiqueta de backup y un tablespace_map en la carpeta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ que ayuda a la recuperación manual.

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 de montaje y los comandos posteriores a la restauración 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 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 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 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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervisar las operaciones de restauración de PostgreSQL

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.

Clonar backups de recursos de PostgreSQL

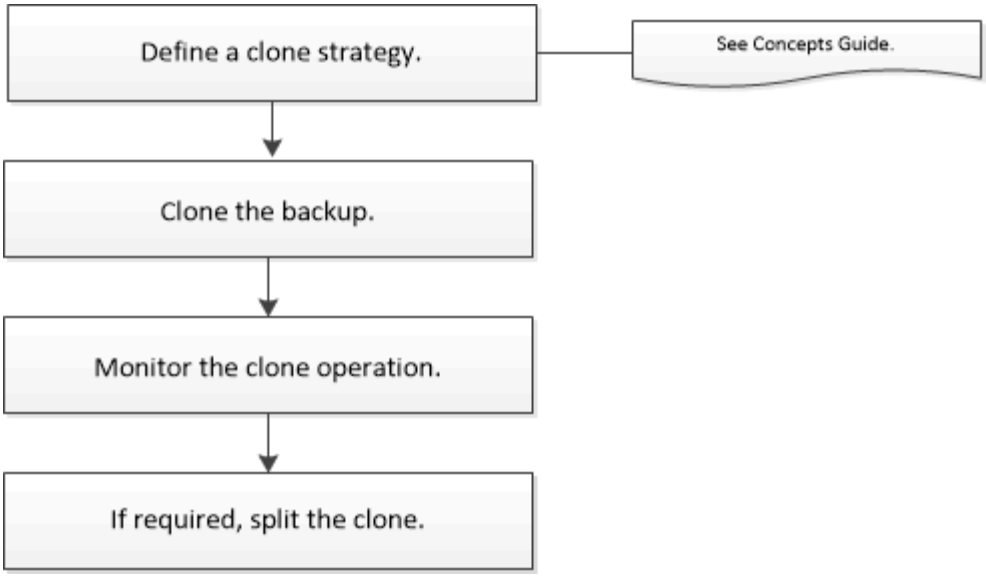
Flujo de trabajo de clonado

El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

Acerca de esta tarea

- Puede clonar en el servidor PostgreSQL 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 PostgreSQL

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario.

Antes de empezar

- 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).
- Para los comandos previos o posteriores a la clonado, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para obtener más información sobre las operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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 Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el servidor	Elija el host donde se debe crear el clon.
Puerto de destino	Introduzca el puerto de destino PostgreSQL para clonar a partir de 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. Esto solo se aplica al recurso de tipo de almacenamiento NFS.
Pool de capacidad máx. Rendimiento (MiB/s)	Introduzca el rendimiento máximo de un pool de capacidad. Esto solo es aplicable a los recursos del tipo de almacenamiento ANF.

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 los clústeres existentes con el mismo nombre
      - Comando posterior a la clonado: Verifique un clúster o inicie un clúster.

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 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.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-SmConnection
```

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 10.32.212.14:

   Para clúster PostgreSQL:

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```

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 clonación de PostgreSQL

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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

Elimine o divida clones de clústeres de PostgreSQL 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 primario de la página Resources.

   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 en para dividir los clones.
7. Haga clic en **Aceptar**.

Proteger MySQL

Complemento de SnapCenter para MySQL

Información general sobre el plugin de SnapCenter para MySQL

El plugin de SnapCenter para bases de datos de MySQL es un compenente del lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de bases de datos de MySQL. El plugin para bases de datos de MySQL automatiza el backup, la restauración y la clonado de bases de datos de MySQL en el entorno de SnapCenter.

SnapCenter admite configuraciones MySQL de instancia única. Es posible utilizar el plugin para base de datos MySQL en entornos Linux y Windows. En entornos Windows, MySQL será soportado como recurso manual.

Cuando se instala el plugin para bases de datos de MySQL, 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.

El complemento de SnapCenter para MySQL es compatible con NFS y SAN en distribuciones de almacenamiento de archivos de ONTAP y Azure NetApp.

Se admite la distribución de almacenamiento virtual VMDK, VVol y RDM.

No se admiten enlaces simbólicos.

Tareas que pueden llevarse a cabo con el plugin de SnapCenter para MySQL

Cuando el plugin para base de datos MySQL está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar instancias MySQL. También es posible ejecutar tareas complementarias a estas operaciones.

- Agregue instancias.
- 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 MySQL

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para base de datos MySQL, 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 instantánea NetApp no disruptiva**

  SnapCenter utiliza la tecnología de snapshots de NetApp con el plugin para bases de datos de MySQL para realizar backups de recursos.

Usar el plugin para MySQL 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 Snapshot del grupo de coherencia (CG) 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 Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear snapshots con comandos externos
- Compatibilidad con LVM de Linux en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el plugin de SnapCenter para MySQL

SnapCenter es compatible con una amplia gama de tipos de almacenamiento tanto en máquinas físicas como máquinas virtuales (VM). Antes de instalar el plugin de SnapCenter para MySQL, debe comprobar la compatibilidad de su tipo de almacenamiento.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • 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. 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. • LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creado • Volúmenes NFS conectados directamente con el Guest VM • Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP requeridos para el plugin de MySQL

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 9.12.1 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - lun
  - lun create
  - lun create
  - lun create

- eliminación de lun
- igroup de lun añadido
- crear lun igroup
- lun igroup eliminado
- cambio de nombre de lun igroup
- 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
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
    - modificación de snapshot de volumen: snaplock: tiempo de caducidad
    - 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
    - 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 8.3.0 y versiones posteriores
    - interfaz de red

- se muestra la interfaz de red
- vserver

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para MySQL

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.

SnapCenter realiza las actualizaciones a SnapMirror y SnapVault después de que finaliza la operación de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.

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 MySQL

Defina una estrategia de backup para MySQL

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 Snapshot consistentes con las aplicaciones de la base de datos.
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 snapshots en el sistema de almacenamiento de origen y el destino de SnapMirror.
7. 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 instancias de MySQL en el host Linux que gestiona SnapCenter. Después de instalar el plugin de SnapCenter para MySQL, las instancias de MySQL en ese host Linux se detectan automáticamente y se muestran en la página Resources.

Tipo de backups admitido

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite el tipo de backup basado en copias de Snapshot para bases de datos MySQL.

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 MySQL.

Cómo utiliza el plugin de SnapCenter para MySQL snapshots de grupos de consistencia

Es posible usar el plugin para crear copias Snapshot de grupos de coherencia 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 coherencia es un conjunto de snapshots 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 snapshot de grupos consistentes. La sincronización WAFL mejora el rendimiento de una snapshot de grupo de coherencia.

Cómo hace SnapCenter para gestionar el mantenimiento de backups de registros

SnapCenter gestiona el mantenimiento de los backups de datos en los niveles de sistema de almacenamiento y sistema de archivos.

Consideraciones para determinar programaciones de backup para MySQL

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 MySQL

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 el plugin para bases de datos MySQL

Es posible usar la convención de nomenclatura de Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la Snapshot.

Estrategia de restauración y recuperación para MySQL

Defina una estrategia de restauración y recuperación para recursos de MySQL

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar una base de datos.

Sólo se admite la recuperación manual de la base de datos.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos de MySQL añadidos manualmente
2. Determinar las estrategias de restauración compatibles con las bases de datos MySQL detectadas automáticamente
3. Decidir el tipo de operaciones de recuperación que se desea ejecutar.

Tipos de estrategias de restauración compatibles con los recursos de MySQL 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 MySQL añadidos manualmente.

No se pueden recuperar recursos MySQL añadidos manualmente.

Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, las copias de Snapshot tomadas después de la copia de Snapshot seleccionada para restaurar en 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.

Tipo de estrategia de restauración compatible con MySQL detectado automáticamente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter.

La restauración de recursos completa es la estrategia de restauración admitida en las bases de datos MySQL detectadas automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para el MySQL autodetectado

El plugin de SnapCenter para MySQL es compatible con SnapRestore de archivos

únicos, y los tipos de restauración por conexión y copia para las bases de datos MySQL detectadas automáticamente.

Single File SnapRestore se realiza en entornos NFS en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- Cuando la copia de seguridad seleccionada se realiza desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **completar recurso**

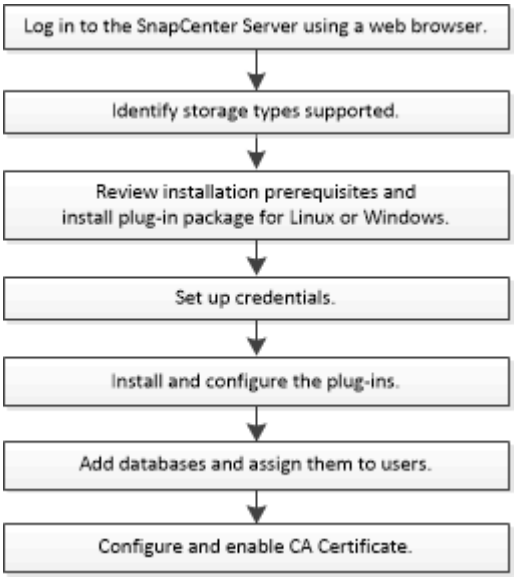
Single File SnapRestore se realiza en entornos SAN en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- Cuando se selecciona la copia de seguridad de una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Complete Resource**

Prepare la instalación del plugin de SnapCenter para MySQL

Flujo de trabajo de instalación del plugin de SnapCenter para MySQL

Tendrá que instalar y configurar el plugin de SnapCenter para MySQL si desea proteger las bases de datos MySQL.



Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para MySQL

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. Plugin SnapCenter para MySQL está disponible en entornos Windows y Linux.

- Debe haber instalado Java 11 en el host.

IBM Java no es compatible con el host Windows y Linux.

- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows 'LocalSystem', que es el comportamiento predeterminado cuando el plugin para MySQL se instala como administrador de dominio.
- 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 MySQL en hosts de Windows.
- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host de MySQL.
- Para MySQL 5,7, binlog debe especificarse en el archivo mysql config (my.cnf o mysql-server.cnf).
- Si utiliza una versión de MySQL anterior a la 8.0, deberá instalar y habilitar manualmente el complemento MySQLX. El complemento MySQLX viene instalado y habilitado de forma predeterminada en MySQL 8.0 y versiones posteriores.

Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Mientras se instala el plugin para MySQL en un host de 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 11 en el host de Windows.

  "Descargar JAVA para todos los sistemas operativos"

Hosts Linux

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

  "Descargar JAVA para todos los sistemas operativos"

- Para bases de datos MySQL que se ejecutan en un host Linux, cuando se instala el plugin para MySQL, el plugin de SnapCenter para UNIX se instala de forma automática.
- Debe tener **bash** como shell por defecto para la instalación del plug-in.

Comandos suplementarios

Para ejecutar un comando complementario en el plugin de SnapCenter para MySQL, debe incluirlo en el archivo *allowed_commands.config*.

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementarios en el host del plugin, abra el archivo *allowed_commands.config* en un editor. Escriba cada comando en una línea diferente y los comandos no distinguen mayúsculas de minúsculas.

Asegúrese de especificar el nombre de ruta completamente cualificado y escribirlo entre comillas si contiene espacios.

Por ejemplo:

Comando: Comando de montaje: Comando umount: C:\Program Files\NetApp\SnapCreator commands\sdcli.exe. myscript.bat

Si el archivo *allowed_commands.config* no está presente, los comandos o la ejecución del script se bloquearán y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

Si el comando o script no está presente en *allowed_commands.config*, el comando o la ejecución del script se bloqueará y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

No debe utilizar una entrada comodín (*) para permitir todos los comandos.

Configure privilegios sudo para usuarios que no son raíz para el host Linux

SnapCenter permite que un usuario no raíz instale el paquete de plugins de SnapCenter para Linux e inicie el proceso del plugin. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro deben tener permiso de 555. De lo contrario, se puede producir un error en la instalación del plugin.
- Para el usuario que no es root, asegúrese de que el nombre del usuario que no es root y del grupo del usuario debe ser el mismo.
- 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/*LINUX_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 HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- _C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ si el servidor SnapCenter está instalado en el host de Windows.
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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 Para obtener la información más reciente sobre las versiones compatibles, consulte la "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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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 • SUSE Linux Enterprise Server (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "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 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	Java 11 Oracle Java y OpenJDK 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.

Configure credenciales para el plugin de SnapCenter para MySQL

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 Settings, haga clic en **Credential**.
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.
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • 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* • 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* 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.

Para este campo…	Realice lo siguiente…
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. Aplicable únicamente a usuarios Linux.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, se recomienda asignar el mantenimiento de credenciales a un usuario o un grupo de usuarios en la página User and Access.

Instale el plugin de SnapCenter para MySQL

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 el host e instalar paquetes de plugins para un host individual.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- 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.

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: • Windows • Linux El plugin para MySQL debe instalarse en el servidor de bases de datos de MySQL.
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.
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. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado. 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.

   Mientras utiliza la API de REST para instalar el plugin para MySQL, debe pasar la versión como 3,0. Por ejemplo, MySQL:3,0

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. 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 MySQL está instalado en el host de cliente MySQL, y este host puede estar en un sistema Windows o Linux. • 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. • Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta.
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.
Añada todos los hosts del clúster	No aplicable.
Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in	No aplicable.

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.

9. Supervise el progreso de la instalación.
   - Para el plugin de Windows, los registros de instalación y actualización se encuentran en: *C:\Windows\SnapCenter plugin\Install*<JOBID>_
   - Para el plugin de Linux, los registros de instalación se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ y los registros de actualización se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Después de terminar

Si desea actualizar a la versión de SnapCenter 6,0, el plugin existente basado en PERL para MySQL se desinstalará del servidor de plugins remoto.

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.

Antes de empezar

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*. Alternativamente, 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.

4. Introduzca sus credenciales para la instalación remota.

Instale el plugin de SnapCenter para MySQL en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para base de datos MySQL 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 MySQL en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

Antes de empezar

- Debe instalar el plugin para base de datos MySQL en cada host Linux donde se debe proteger la instancia de MySQL.
- El host Linux en el que se instala el plugin de SnapCenter para base de datos MySQL debe cumplir con los requisitos dependientes de software, base de datos y sistema operativo.

  El "Herramienta de matriz de interoperabilidad (IMT)" Contiene la información más reciente sobre las configuraciones compatibles.

- El plugin de SnapCenter para base de datos MySQL 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 archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar el plugin para MySQL.

   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. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y, a continuación, añada el parámetro PLUGINS_ENABLED = MySQL:3,0.

5. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervise el estado de instalación del plugin para MySQL

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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configure el certificado de CA para el servicio de plugins de MySQL de SnapCenter en el host Linux

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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 del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento: /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 para complementar el almacén de confianza.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento /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 del almacén de claves del complemento predeterminado es el valor de la clave 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 firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para complementos

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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 de MySQL de SnapCenter en el host Windows

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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*.

4. Reinicie el servicio después de cambiar la contraseña.

   La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 para complementar el almacén de confianza.

   Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 del almacén de claves del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos 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 de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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.

Antes de empezar

- 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*. Alternativamente, 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 el plugin de SnapCenter para MySQL

Antes de utilizar el plugin de SnapCenter para MySQL, el administrador de SnapCenter debe haber instalado y configurado SnapCenter Server y ejecutado 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 11 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.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger MySQL

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 instancias de MySQL 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.

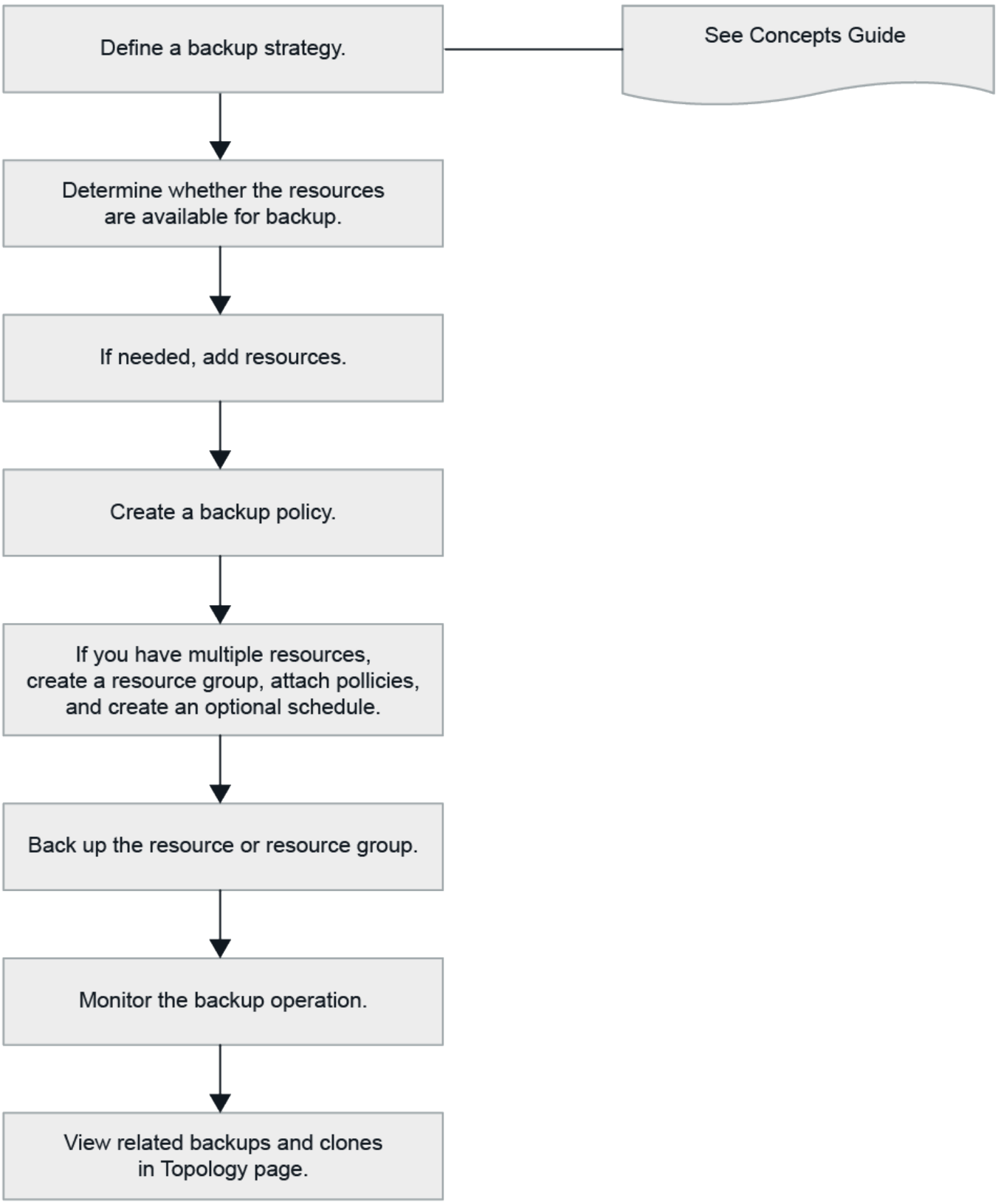
Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos 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.

Realizar backup de recursos de MySQL

Realizar backup de recursos de MySQL

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. "Guía de referencia de cmdlets de SnapCenter Software".

Detectar las bases de datos automáticamente

Los recursos son bases de datos MySQL en el host Linux gestionados por SnapCenter. Es posible añadir los recursos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos MySQL disponibles.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts y configurar las conexiones del sistema de almacenamiento.
- El plugin de SnapCenter para MySQL no es compatible con la detección automática de los recursos que residen en los entornos virtuales de 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, se detectan automáticamente todas las bases de datos en ese host Linux y se muestran en la página Resources.
- Solo se detectan automáticamente las bases de datos.

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, a continuación, seleccione el plugin para MySQL de la lista.
2. En la página Resources, seleccione el tipo de recurso en la lista View.
3. (Opcional) Haga clic en y 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.

Debe actualizar los recursos si se cambia el nombre de las instancias fuera de SnapCenter.

Añada recursos manualmente al host del plugin

El host Windows no admite la detección automática. Debe añadir manualmente las instancias y los recursos de la base de datos de MySQL.

Antes de empezar

- Debe haber completado tareas como instalar SnapCenter Server, añadir hosts y configurar conexiones del sistema de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, seleccione el plugin de SnapCenter para MySQL en la lista desplegable y, a continuación, haga clic en * Recursos *.
2. En la página Recursos, haga clic en **Agregar recursos MySQL**.
3. En la página Provide Resource Details, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre	Especifique el nombre de la base de datos.
Nombre de host	Introduzca el nombre de host.
Tipo	Seleccione Instance.
Instancia	No aplicable
Credenciales	Seleccione las credenciales o agregue información para la credencial. Esto es opcional.

4. En la página Provide Storage Footprint, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees y, 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. Opcional: En la página Resource Settings, introduzca pares personalizados de clave-valor para el plugin de MySQL.
6. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Las bases de datos se muestran junto con información como el nombre del host, las políticas y los 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 MySQL.

Crear políticas de backup para MySQL

Antes de usar SnapCenter para realizar un backup de recursos de MySQL, 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.

Antes de empezar

- Debe tener definida una estrategia de backup.

  Para obtener detalles, consulte la información sobre cómo definir una estrategia de protección de datos para bases de datos MySQL.

- 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 snapshots 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.

Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de instantáneas, se evita la eliminación de las instantáneas hasta que caduque el período de retención. Esto podría provocar que se retenga un número mayor de instantáneas que el recuento especificado en la política.
  - Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 sus detalles.
5. En la página Policy type, realice lo siguiente:
   a. Seleccione el tipo de almacenamiento.
   b. En la sección Custom backup settings, proporcione cualquier configuración de backup específica que tenga que pasarse al plugin en formato de clave-valor.

      Puede pasar varios pares de clave-valor al plugin.

6. En la página Snapshot and Replication, realice los siguientes pasos:

   a. 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.

a. En la sección Configuración de instantánea, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionado en la página **Tipo de copia de seguridad**:

Si desea…	Realice lo siguiente…
Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino. El valor de retención máximo es 1018. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y especifique días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

b. Seleccione una etiqueta de política.

Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

7. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

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). Si la relación en ONTAP es del tipo Reflejo y almacén y solo se selecciona esta opción, Snapshot creado en el origen no se transferirá al destino, pero figurará en el destino. Si esta copia 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. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Consulte "Consulte los backups y los clones relacionados con los recursos de MySQL en la página Topology".

Para este campo…	Realice lo siguiente…
Actualizar SnapVault después de crear una copia Snapshot local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el almacén de SnapLock, consulte Confirmar instantáneas en WORM en un almacén destino Consulte "Consulte los backups y los clones relacionados con los recursos de MySQL en la página Topology".
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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

8. 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.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad

de SnapLock.

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 los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. 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.
Use 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 snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la snapshot.

4. En la página Resources, 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.

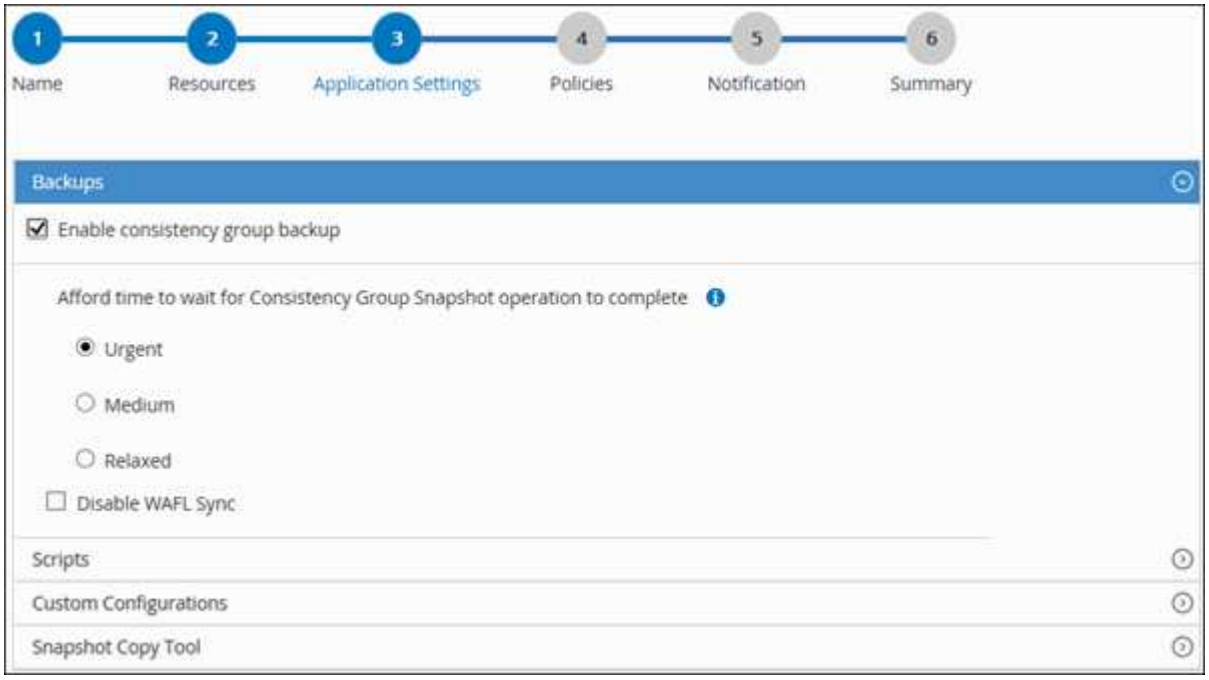
5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. En la página Application Settings, realice lo siguiente:

   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…
Espere tiempo a que finalice la operación de snapshot de grupo de consistencia	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que se complete la operación de instantánea. 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 PRE y POST para las operaciones de inactividad, instantánea y desactivación. 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. 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. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.16151855 1942 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. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

Los pares de clave-valor personalizados son compatibles con los sistemas de plugins MySQL Linux y no son compatibles con la base de datos MySQL registrada como un plugin de Windows centralizado.

c. Haga clic en la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

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**.
SnapCenter para crear una snapshot a 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 **Otro** y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

7. 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 + .

      Las políticas figuran en la sección Configure schedules for selected policies.

   b. En la columna Configure Schedules, haga clic en + en la política 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.

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. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

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

Cree grupos de recursos y habilite la protección secundaria para recursos de MySQL en sistemas R2 de ASA

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario

y secundario, el grupo de recursos se queda sin modo de mantenimiento.

- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:
   a. Seleccione el tipo de política de replicación.

      No se admite la política de replicación síncrona.

   b. Especifique el sufijo del grupo de consistencia que desea utilizar.
   c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

      SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para MySQL

Es necesario 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 MySQL.

Antes de empezar

- 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 Core mediante el cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

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 MySQL a SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode mysql
```

5. Instale el paquete y el plugin de SnapCenter para MySQL en el host.

   Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
mysql
```

   Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina la ruta de acceso a SQLLIB.

   Para Windows, el plugin de MySQL utilizará la ruta predeterminada para la carpeta SQLLIB: “C:\Program Files\IBM\SQLLIB\BIN”

   Si desea anular la ruta predeterminada, utilice el comando siguiente.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{“MySQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

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

Hacer backup de MySQL

Si un recurso aún no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

Antes de empezar

- 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 la operación de backup basado en copias de Snapshot, asegúrese de que todas las bases de datos de tenant sean válidas y estén activas.
- Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y la reanudación de la copia, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin con las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

UI de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Seleccione * * y, a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede seleccionar cerrar el panel de filtros.
3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.
5. En la página Application Settings, realice lo siguiente:

   - Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales:

     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

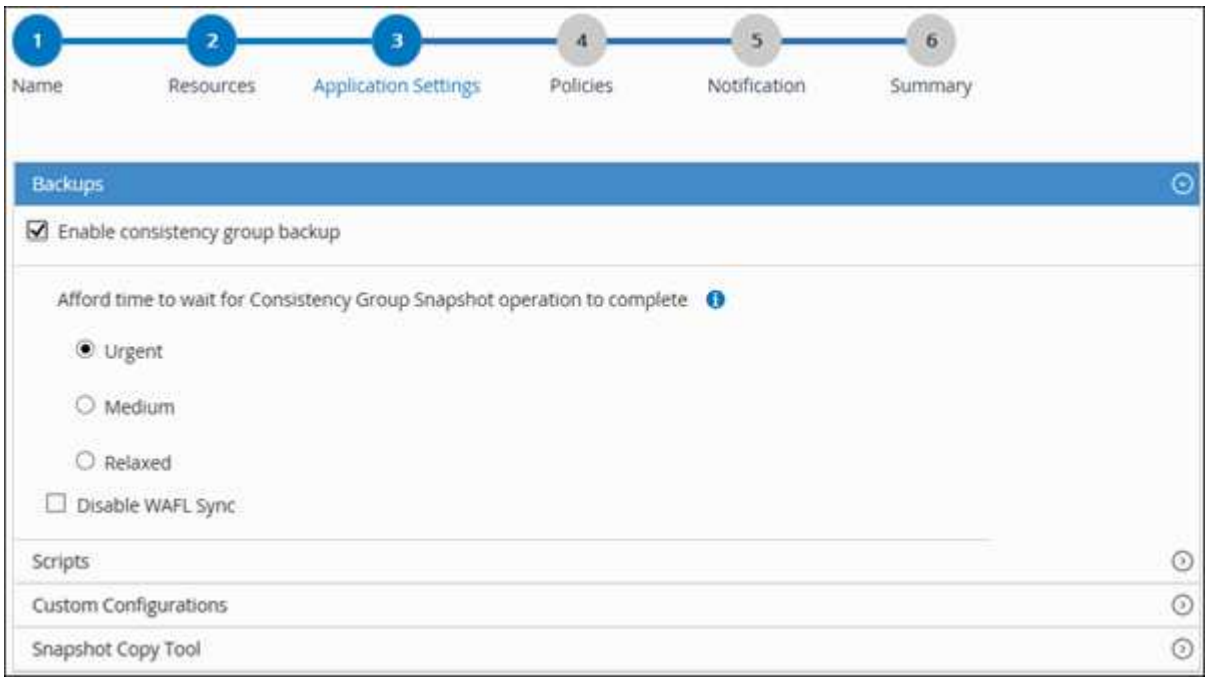
Para este campo…	**Realice lo siguiente…**
Permitir que se complete la operación de "Snapshot de grupo de consistencia"	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que finalice la operación de instantánea. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.

   - Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.

     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.
   - Seleccione la flecha **Configuraciones personalizadas**y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
   - Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	**Realice lo siguiente…**
SnapCenter cree una snapshot a 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**.
Para escribir el comando para crear una snapshot	Seleccione **Otro** y luego ingrese el comando para crear una instantánea.



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. Seleccione + en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

      policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

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. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

8. Revisa el resumen y luego selecciona **Finalizar**.

   Se muestra la página de topología de los recursos.

9. Seleccione **Back up Now**.
10. En la página Backup, 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. Seleccione **copia de seguridad**.
11. 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*

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\
   ```

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada recursos manuales mediante el cmdlet Add-SmResources.

   Este ejemplo muestra cómo agregar una instancia de MySQL:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
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 -Resources
   @{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
   luginName"="MySQL"} -Policy "MySQL_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 mysql_policy2
   ```

6. Supervise el estado de la tarea (running, completed o failed) mediante el cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

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.

Antes de empezar

- 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 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, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos escribiendo su nombre en el cuadro de búsqueda o seleccionando y, luego, seleccionar la etiqueta. A continuación, puede seleccionar cerrar el panel de filtros.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **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. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Supervisar las operaciones de backup de MySQL

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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 las instancias de MySQL 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Cancelar las operaciones de backup para MySQL

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. 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 de MySQL 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, 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.

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 del número de copias de seguridad y clones disponibles en el almacenamiento principal y secundario.

   La sección **Summary Card** muestra el número total de copias de Snapshot y clones.

   Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Después de la copia de seguridad a petición, haciendo clic en el botón **Actualizar** actualiza los detalles de la copia de seguridad o clonación.

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 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.

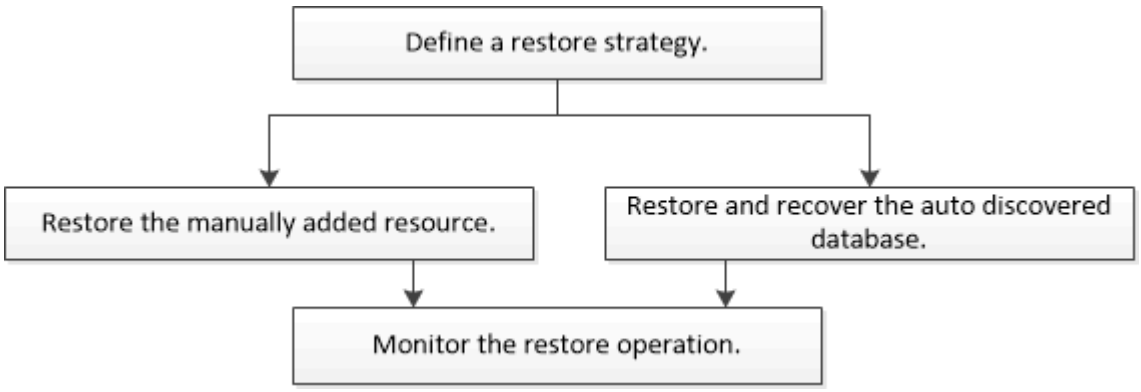
7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
8. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Restaure MySQL

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.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para ONTAP 9.12,1 y versiones anteriores, los clones creados a partir de las snapshots de SnapLock Vault como parte de la restauración heredarán el tiempo de caducidad del almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad

de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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.

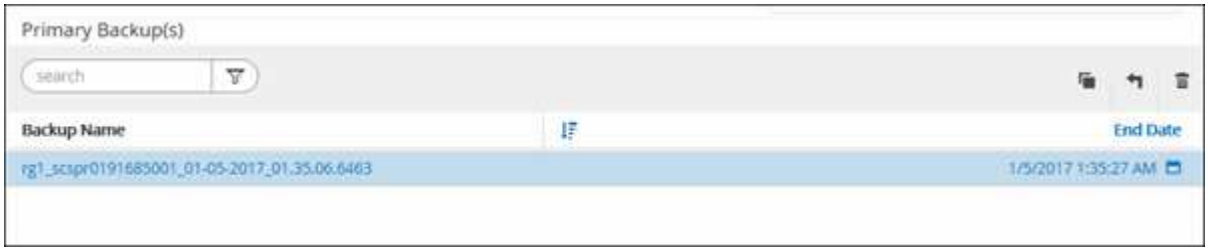
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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**.

   a. Si selecciona **Recurso completo**, se restauran todos los volúmenes de datos configurados de la base de datos MySQL.

      Si el recurso contiene volúmenes o qtrees, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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.

      Puede seleccionar varios LUN.

      Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.

7. 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.

8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

9. 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 la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Restaurar y recuperar un backup de base de datos detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- 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.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

- Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para los recursos detectados automáticamente, se admite la restauración con SFSR.
- No se admite la recuperación automática puntual y actualizada al minuto.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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, filtre los recursos de la lista desplegable **View** 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.

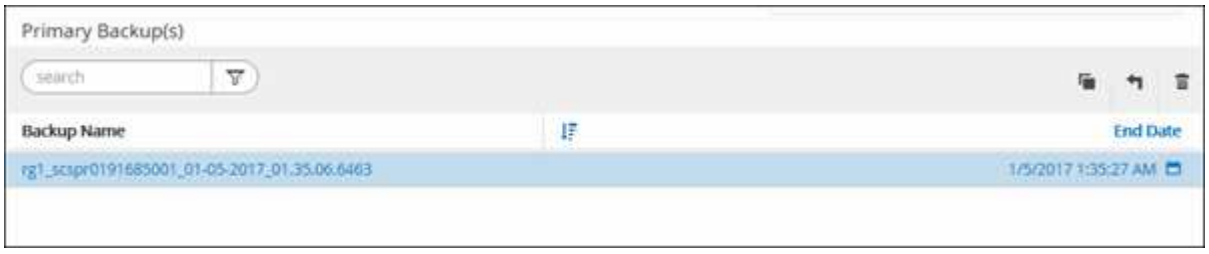
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   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 MySQL.

7. 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.

8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

9. 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 la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervise operaciones de restauración de MySQL

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.

Clonar backups de recursos de MySQL

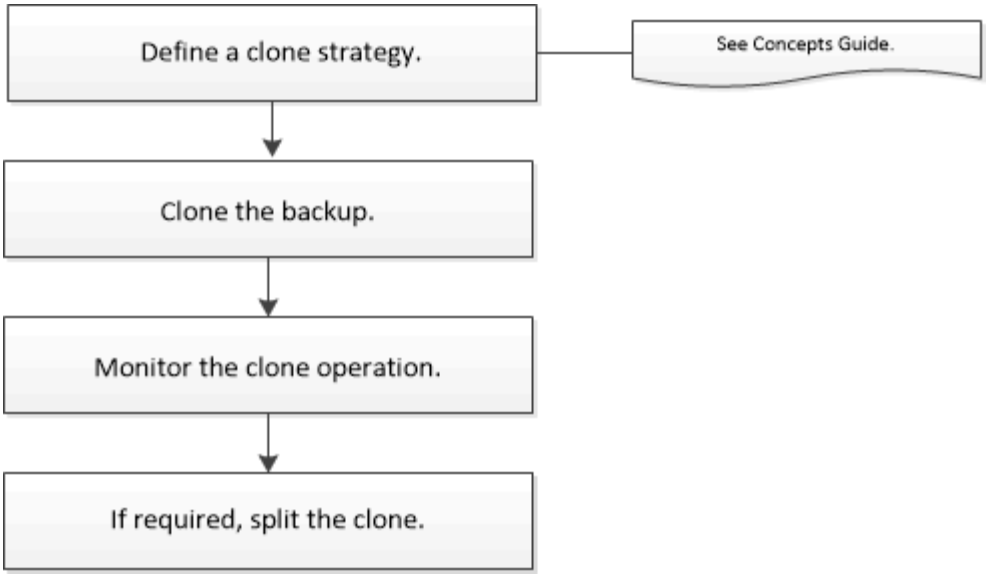
Flujo de trabajo de clonado

El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

Acerca de esta tarea

- Puede clonar en el servidor MySQL 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 MySQL

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario.

Antes de empezar

- 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).
- Para los comandos previos o posteriores a la clonado, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:
  - Ubicación predeterminada en el host de Windows: *C:\Archivos de programa\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Ubicación predeterminada en el host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

> Si no hay comandos en la lista de comandos, se producirá un error en la operación. * Para la versión MySQL 5,7, debe configurar IGNORE_MYSQLX_PORT = true (por defecto false) en el MySQL. archivo de propiedades.

Acerca de esta tarea

- No es posible proteger las instancias de MySQL clonadas.
- Para obtener más información sobre las operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- Para ONTAP 9.12,1 y versiones anteriores, los clones creados a partir de las snapshots de SnapLock Vault como parte de la restauración heredarán el tiempo de caducidad del almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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 Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el servidor	Elija el host donde se debe crear el clon.
Puerto	Proporcione el puerto en el que se iniciará la instancia de MySQL clonada.
Dirección IP de exportación NFS	Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados.

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 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.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> 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 10.32.212.14:

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName
"scs000211748_gdl_englab_netapp_com_MySQL_mysqld_3306_scs000211748_0
6-26-2024_06.08.35.4307" -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306"}
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```

   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 clonación de MySQL

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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

Elimine o divida clones de base de datos MySQL 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 primario de la página Resources.

   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 en para dividir los

clones.

7. Haga clic en **Aceptar**.

Proteger aplicaciones mediante los complementos compatibles con NetApp

Complementos compatibles con NetApp

Información general sobre los plugins compatibles de NetApp

Es posible usar los complementos compatibles con NetApp, como MongoDB, ORASCPM (aplicaciones Oracle), SAP ASE, SAP MaxDB y el complemento de almacenamiento para aplicaciones que se usen y, a continuación, utilizar SnapCenter para realizar backups, restaurar o clonar tales aplicaciones. Los plugins compatibles con NetApp funcionan como componentes del host del software NetApp SnapCenter y permiten la protección de datos para aplicaciones y la gestión de recursos.

Cuando se instalan plugins compatibles con NetApp, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp 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 compatibles con NetApp se pueden utilizar tanto en entornos de Windows como de Linux.

SnapCenterCLI no admite comandos de plugins compatibles con NetApp.

NetApp proporciona el complemento de almacenamiento para realizar operaciones de protección de datos del volumen de datos en el almacenamiento ONTAP utilizando el marco de complemento integrado en SnapCenter.

Puede instalar los plugins compatibles con NetApp desde la página Add Host.

"Añada hosts e instale paquetes de plugins en hosts remotos."

La política de soporte de SnapCenter abarcará la compatibilidad con el framework de complementos, el motor principal y las API asociadas. No se incluirá el código fuente del complemento ni los scripts asociados creados en el framework de complementos.

Tareas que pueden llevarse a cabo con los plugins compatibles con NetApp

Es posible usar los complementos compatibles con NetApp, como MongoDB, ORASCPM, aplicaciones Oracle, SAP ASE, SAP MaxDB y el complemento de almacenamiento para 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.

Es posible usar los plugins compatibles con NetApp para las operaciones de protección de datos.

- Realice copias Snapshot de grupo de coherencia de los volúmenes de almacenamiento en los clústeres de ONTAP.
- Realice copias de seguridad de aplicaciones personalizadas mediante el marco incorporado de secuencias de comandos previas y posteriores

  Es posible realizar backups de un volumen de ONTAP, LUN o un qtree.

- Actualice las snapshots creadas del almacenamiento primario a un secundario de ONTAP aprovechando la relación de replicación existente (SnapVault/SnapMirror/replicación unificada) mediante la normativa de SnapCenter

  ONTAP primario y secundario puede ser ONTAP FAS, AFF, ASA, ONTAP Select o Cloud Volumes ONTAP.

- Recupere volúmenes, LUN o archivos ONTAP completos.

  Debe proporcionar la ruta de archivo correspondiente manualmente, ya que las funciones de exploración o indexación no están integradas en el producto.

  No se admite la restauración de qtree o directorio, pero solo se puede clonar y exportar el qtree si el alcance de backup se define en el nivel de Qtree.

Las funciones de los plugins compatibles con NetApp

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con los complementos compatibles con NetApp, como MongoDB, ORASCPM (Aplicaciones Oracle), SAP ASE, SAP MaxDB y el complemento de almacenamiento, 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 NetApp instantánea no disruptiva**

  SnapCenter utiliza la tecnología Snapshot de NetApp con los complementos compatibles con NetApp para realizar backups de recursos. Las snapshots consumen un espacio de almacenamiento mínimo.

Los complementos compatibles con NetApp además ofrecen 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 Snapshot del grupo de consistencia (CG) 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 Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear Snapshot con comandos externos
- Capacidad para crear snapshots consistentes con el sistema de archivos en entornos Windows

Tipos de almacenamiento admitidos por los plugins compatibles con NetApp

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 compatibles con NetApp.

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
Montajes físicos y directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM).	LUN conectados a iSCSI
Montajes físicos y directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM).	Volúmenes conectados en NFS
VMware ESXi	Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP requeridos para el plugin compatible con NetApp

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 9.12.1 y versiones posteriores

- event generate-autosupport-log
- se muestra el historial del trabajo
- detención de trabajo
- se muestra el atributo de lun
- lun create
- eliminación de lun
- geometría 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
- interfaz de red
- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- 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
- 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 8.3.0 y versiones posteriores
  - interfaz de red

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y de SnapVault para complementos compatibles con NetApp

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.

SnapCenter realiza las actualizaciones a SnapMirror y SnapVault después de que finaliza la operación de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.

> 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 snapshots de los grupos de consistencia y elegir las opciones apropiadas para eliminar las snapshots de los grupos de consistencia.
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 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.

La estrategia de backup para complementos compatibles con NetApp

Programaciones de backup de recursos de plugins compatibles con NetApp

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 plugins compatibles con NetApp 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 plugins compatibles con NetApp que se añaden manualmente.

No se pueden recuperar manualmente los recursos de plugins compatibles con NetApp que se añadieron manualmente.

Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, las snapshots realizadas después de la Snapshot seleccionada para restaurar en 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.

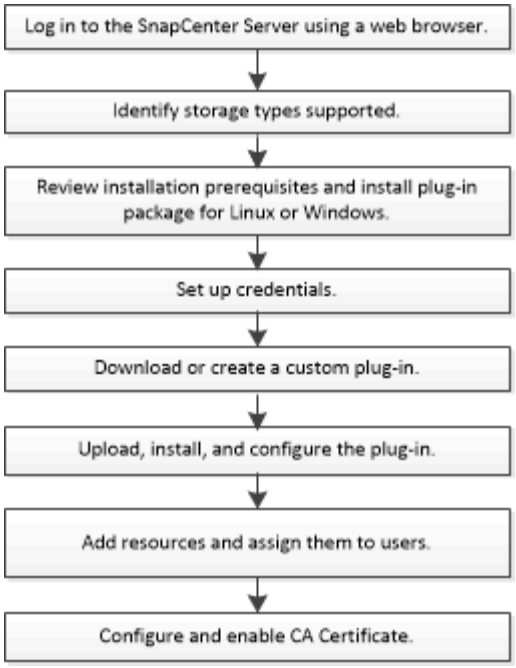
Restauración de nivel de archivos

- Restaura los archivos de volúmenes, qtrees o directorios
- Restaura solo los LUN seleccionados

Preparar la instalación de complementos compatibles con NetApp

Flujo de trabajo de instalación de plugins compatibles con SnapCenter NetApp

Deber instalar y configurar plugins compatibles con SnapCenter NetApp si desea proteger los recursos de plugins compatibles con NetApp.



Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos. Los plugins compatibles con NetApp son compatibles con entornos Windows, Linux y AIX.

El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

- Debe haber instalado Java 11 en el host Linux, Windows o AIX.

  IBM Java no es compatible con el host Windows y Linux.

- 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 complementos compatibles con NetApp, como MongoDB, ORASCPM, aplicaciones Oracle, SAP ASE, SAP MaxDB y el complemento de almacenamiento 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.
- Debe seleccionar manualmente el plugin de SnapCenter para Microsoft Windows.

"Descargar JAVA para Windows"

Hosts Linux y AIX

El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

  Si utiliza Windows Server 2019 o Windows Server 2016 para el host de SnapCenter Server, debe instalar Java 11.

  "Descargar JAVA para Linux"

  "Descargar JAVA para AIX"

- 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.

  Asegúrese de utilizar sudo versión 1.8.7 o posterior.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

  LINUX_USER es el nombre del usuario que no es raíz que ha creado.

  Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

  - *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.

- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux.

  Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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 almacenamiento y las aplicaciones de Oracle son compatibles con 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 7,1 o posterior
RAM mínima para el plugin de SnapCenter en el host	4 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB 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 11 IBM Java 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.

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. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. 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 versión 1.8.7 o posterior.
- 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 HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

AIX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host de Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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 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 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	• ASP.NET Core Runtime 8.0.12 (y todos los parches 8,0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux y AIX

Debe asegurarse de que el host cumpla los requisitos antes de instalar el paquete de plugins de SnapCenter para Linux o AIX.

El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

Elemento	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)

Elemento	Requisitos
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 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 11 Oracle Java u OpenJDK 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 plugins compatibles con NetApp

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.

Antes de empezar

- Hosts Linux o AIX

  Debe configurar credenciales para instalar plugins en hosts Linux o AIX.

  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 complementos compatibles con NetApp

  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 Settings, haga clic en **Credential**.
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. • 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* • 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*
Contraseña	Introduzca la contraseña usada para autenticación.
Tipo de autenticación	Seleccione el tipo de autenticación que desea usar.
Use privilegios sudo	Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz. Aplicable únicamente a usuarios Linux y AIX.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 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>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. 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 complementos compatibles con NetApp

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 los paquetes de los plugins para un host individual o para un clúster.

Antes de empezar

- 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 2016 o posterior para aplicaciones personalizadas"

- Para el host de Windows, debe asegurarse de seleccionar el plugin de SnapCenter para Windows.

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 izquierdo, seleccione **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página hosts, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione el tipo de host: • Windows • Linux • AIX Los plugins compatibles con NetApp se pueden utilizar en entornos de Windows, Linux y AIX. El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.
Nombre de host	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. 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. Puede introducir las direcciones IP o el FQDN de un host independiente. 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. Las credenciales deben tener derechos de administración en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. 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.

   Puede instalar los siguientes plugins de la lista:

   - MongoDB
   - ORASCPM (se muestra como Aplicaciones Oracle)
   - SAP ASE
   - MaxDB de SAP
   - Reducida

6. (Opcional) Seleccione **Más opciones** para instalar los otros plug-ins.

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. 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 compatibles con NetApp pueden instalarse en sistemas Windows o Linux. • 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. • Para el paquete de plugins de SnapCenter para Linux y el paquete de plugins de SnapCenter para AIX, la ruta predeterminada es `/opt/NetApp/snapcenter`. Opcionalmente, puede personalizar la ruta.
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. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows.

7. Seleccione **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, 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 SnapManager.web.ui.dll.config, debe actualizar el archivo en ambos nodos y reiniciar el grupo de aplicaciones de SnapCenter.

La ruta predeterminada de Windows es `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

La ruta predeterminada de Linux es `/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

8. Si el tipo de host es Linux, verifique la huella dactilar y, a continuación, seleccione **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.

9. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación se encuentran en `/custom_location/snapcenter/` registros.

Instale paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

Antes de empezar

El usuario que agrega un host debe tener derechos administrativos en el host.

El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

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*. Alternativamente, 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.

4. Introduzca sus credenciales para la instalación remota.

Instale los plugins compatibles con NetApp en los hosts Linux mediante la interfaz de línea de comandos

Debe instalar los plugins compatibles de NetApp 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 complementos compatibles con NetApp en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

Pasos

1. Copie el archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar los plugins compatibles de NetApp.

   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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

5. Inicie sesión en SnapCenter y cargue el plugin compatible con NetApp desde la interfaz de usuario de o mediante cmdlets de PowerShell.

   En la sección, puede cargar el plugin compatible con NetApp desde la interfaz de usuario "Añada hosts e instale paquetes de plugins en hosts remotos" .

   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 instalación de los plugins compatibles con NetApp

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 solo se enumeren las operaciones de instalación de 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.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

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 se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.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”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host Linux

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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 del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento: /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 para complementar el almacén de confianza.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento /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 del almacén de claves del complemento predeterminado es el valor de la clave 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 firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para complementos

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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 compatibles con NetApp en el host de Windows

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

   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*.

4. Reinicie el servicio después de cambiar la contraseña.

   La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 para complementar el almacén de confianza.

   Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

Debe configurar el par de claves firmadas por CA en el almacén de confianza del complemento.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\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 del almacén de claves del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos 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 de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos 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.

Antes de empezar

- 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*. Alternativamente, 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 compatibles de NetApp

Antes de usar plugins compatibles con SnapCenter NetApp, 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 11 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 rutas de datos (LIF) en SVM, SnapCenter elige la ruta de datos (LIF) adecuada para montar el volumen clonado NFS. Sin embargo, si desea especificar una ruta de datos específica (LIF), debe ejecutar la CLI Set-SvmPreferredDataPath. La información sobre los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, 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 compatibles con NetApp, 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 plugins compatibles con NetApp

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

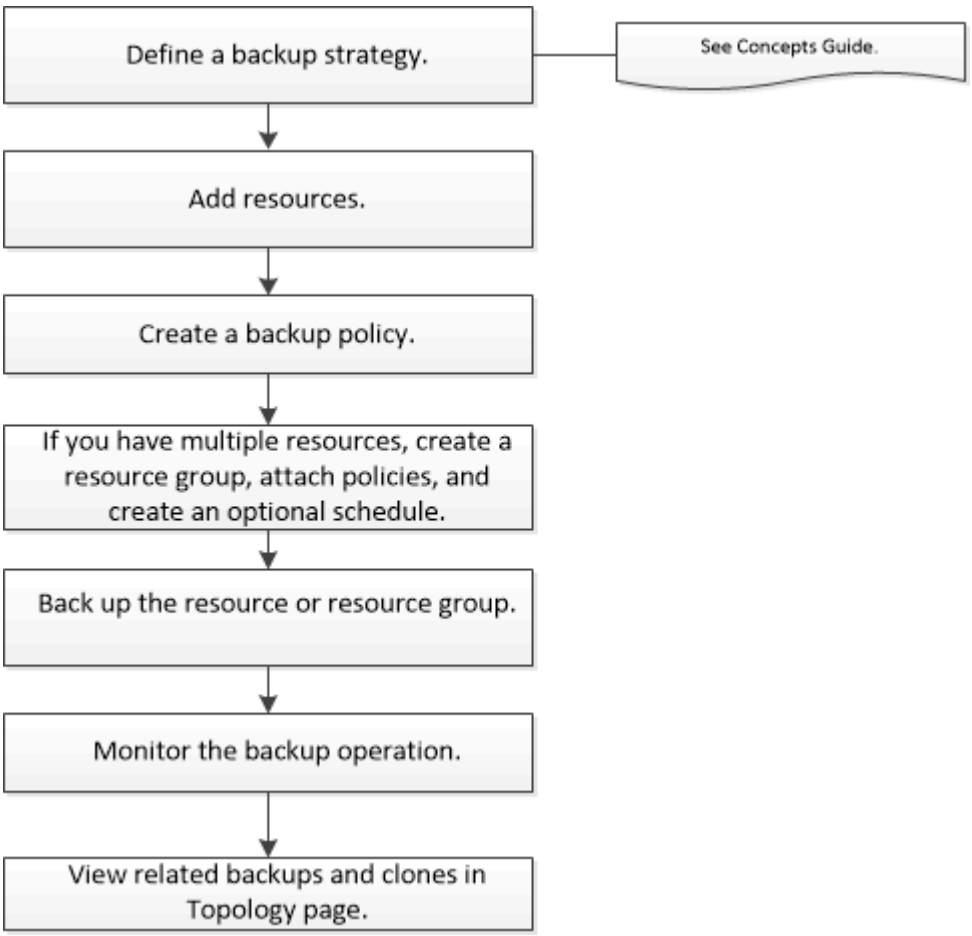
recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando crea el grupo de recursos y añade las políticas, puede configurar el grupo de recursos para que ejecute un backup diario basado en archivos y otra programación que ejecute un backup por hora basado en Snapshot.

Realizar backup de los recursos de plugins compatibles con NetApp

Realizar backup de los recursos de plugins compatibles con NetApp

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 la "Guía de referencia de cmdlets de SnapCenter Software"

Añada recursos a los plugins compatibles con NetApp

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.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir credenciales.
- Debe haber cargado los plugins en SnapCenter Server.

Pasos

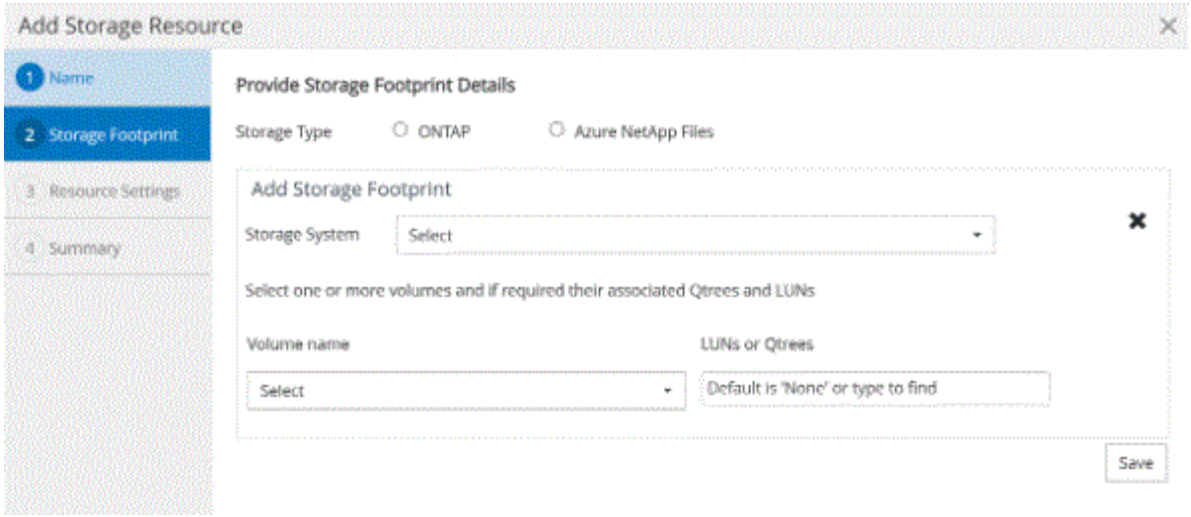
1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, selecciona **Agregar recurso**.
3. En la página Provide Resource Details, realice las siguientes acciones:

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. 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 y, a continuación, seleccione **Save**.

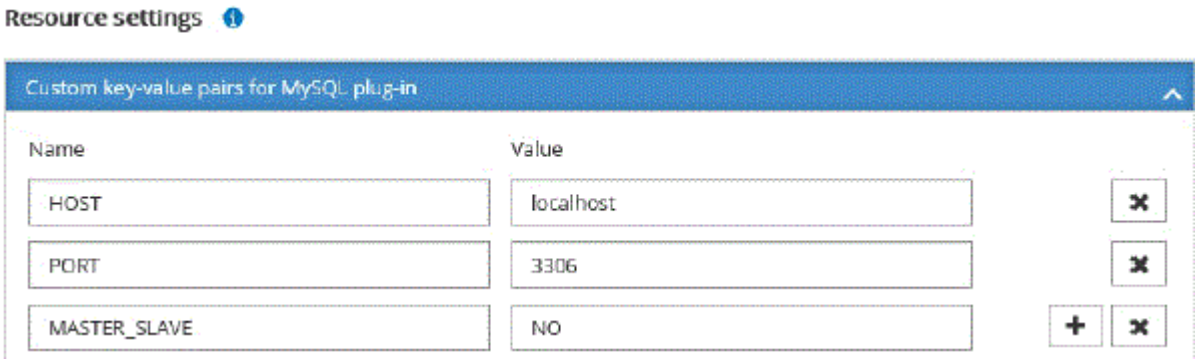
   Opcional: Seleccione la Icono para añadir más volúmenes, LUN y qtrees desde otros sistemas de almacenamiento.

   Los plugins compatibles con NetApp no admiten la detección automática de los recursos. Los detalles de almacenamiento de entornos físicos y virtuales también no se detectan automáticamente. Debe proporcionar la información de almacenamiento de los entornos físico y virtual durante la creación de los recursos.



5. En la página Resource Settings, proporcione pares personalizados de clave-valor para el recurso.

   Asegúrese de que el nombre de las claves personalizadas está en mayúsculas.



   Para conocer los parámetros de conexión correspondientes, consulte "Parámetros para configurar el recurso"

6. Revisa el resumen y luego selecciona **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.

Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

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 plugins compatibles con NetApp tiene backups asociados, los siguientes campos no se pueden modificar: Nombre del recurso, tipo de recurso y nombre de host.

Parámetros para configurar el recurso

Si va a añadir los plugins manualmente, puede utilizar los siguientes parámetros para configurar el recurso en la página Resource Settings.

Plugin para MongoDB

Configuración del recurso:

- MONGODB_APP_SERVER=(para el tipo de recurso como cluster compartido) o MONGODB_REPLICASET_SERVER=(para el tipo de recurso como replicaset)
- OPLOG_PATH=(Parámetro opcional en caso de que se proporcione desde MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN para la autenticación LDAP y Ninguno para otros)

Debe proporcionar los siguientes parámetros n archivo MongoDB.properties:

- DISABLE_START_STOP_SERVICES=
  - N si el plugin realiza los servicios start/stop.
  - Si el usuario realiza los servicios START/**STOP.
  - El parámetro opcional como valor predeterminado se establece en N.
- OPLOG_PATH_= (Parámetro opcional en caso de que ya se haya proporcionado como par clave-valor personalizado en SnapCenter).

Plugin para MaxDB

Configuración del recurso:

- XUSER_ENABLE (Y|N) activa o desactiva el uso de un xuser para MaxDB para que no se necesite una contraseña para el usuario de la base de datos.
- HANDLE_LOGWRITER (Y|N) ejecuta operaciones de suspensión del escritor de registro (N) o reanudación del escritor de registro (Y).
- DBMCLICMD (path_to_dbmcli_cmd) especifica la ruta al comando dbmcli de MaxDB. Si no se define, se utiliza dbmcli en la ruta de búsqueda.

  En el caso de entornos Windows, la ruta debe estar entre comillas dobles ('…').

- SQLCLICMD (path_to_sqlcli_cmd) especifica la ruta al comando sqlcli de MaxDB. Si la ruta de acceso no está definida, sqlcli se utiliza en la ruta de búsqueda.
- MAXDB_UPDATE_HIST_LOG (Y|N) indica al programa de copia de seguridad de MaxDB si debe actualizar el registro del historial de MaxDB.
- MAXDB_CHECK_SNAPSHOT_DIR : example, SID1:directory[,directory…]; [SID2:directoary[,directory…] Comprueba que una operación de copia de Snapshot de Snap Creator se realice correctamente y garantiza que se cree la snapshot.

  Esto se aplica únicamente a NFS. El directorio debe apuntar a la ubicación que contiene el directorio .snapshot. Se pueden incluir varios directorios en una lista separada por comas.

  En MaxDB 7.8 y versiones posteriores, la solicitud de backup de base de datos se Marca con errores en el historial de backup.

- MAXDB_BACKUP_TEMPLATES: Especifica una plantilla de copia de seguridad para cada base de datos.

  La plantilla debe existir y ser un tipo externo de plantilla de copia de seguridad. Para habilitar la integración de instantáneas para MaxDB 7,8 y posterior, debe tener la funcionalidad de servidor en segundo plano de MaxDB y la plantilla de copia de seguridad de MaxDB ya configurada del tipo EXTERNO.

- MAXDB_BG_SERVER_PREFIX: Especifica el prefijo para el nombre del servidor en segundo plano.

  Si se establece el parámetro MAXDB_BACKUP_TEMPLATES, también debe establecer el parámetro MAXDB_BG_SERVER_PREFIX. Si no establece el prefijo, se utiliza el valor predeterminado na_bg_.

Plugin para SAP ASE

Configuración del recurso:

- SYBASE_SERVER (DATA_SERVER_NAME) especifica el nombre del servidor de datos Sybase (opción-S en el comando isql). Por ejemplo, p_test.
- SYBASE_DATABASES_EXCLUDE (db_name) permite excluir las bases de datos si se utiliza la construcción “ALL”.

  Puede especificar varias bases de datos con una lista separada por punto y coma. Por ejemplo: pubs2;test_db1.

- SYBASE_USER: User_name especifica el usuario del sistema operativo que puede ejecutar el comando isql.

  Necesario para UNIX. Este parámetro es obligatorio si el usuario que ejecuta los comandos start y stop de Snap Creator Agent (normalmente el usuario raíz) y el usuario que ejecuta el comando isql son diferentes.

- SYBASE_TRAN_DUMP db_name:DIRECTORY_PATH permite realizar un volcado de transacciones de Sybase después de crear una instantánea. Por ejemplo, pubs2:/sybasedumps/ pubs2

  Debe especificar cada base de datos que necesita un volcado de transacciones.

- SYBASE_TRAN_DUMP_COMPRESS (Y|N) activa o desactiva la compresión de volcado de transacciones de Sybase nativa.
- SYBASE_iSQL_CMD (por ejemplo, /opt/sybase/ocs-15_0/bin/isql) define la ruta de acceso al comando isql.
- SYBASE_EXCLUDE_TEMPDB (Y|N) permite excluir automáticamente las bases de datos temporales creadas por el usuario.

Complemento para aplicaciones Oracle (ORASCPM)

Configuración del recurso:

- SQLPLUS_cmd especifica la ruta a sqlplus.
- ORACLE_DATABASES muestra las bases de datos de Oracle de las que se debe realizar un backup y el usuario correspondiente (database:user).
- CNTL_FILE_BACKUP_DIR especifica el directorio para la copia de seguridad del archivo de control.
- ORA_TEMP especifica el directorio de los archivos temporales.
- ORACLE_HOME especifica el directorio en el que está instalado el software de Oracle.

- ARCHIVE_LOG_ONLY especifica si se realizará o no el backup de los registros de archivos.
- ORACLE_BACKUPMODE especifica si se debe realizar una copia de seguridad en línea o fuera de línea.
- ORACLE_EXPORT_PARAMETERS especifica si las variables de entorno definidas anteriormente deben reexportarse al ejecutar */bin/su <user running sqlplus> -c sqlplus /nolog <cmd>*. Esto suele ocurrir cuando el usuario que ejecuta sqlplus no ha configurado todas las variables de entorno necesarias para conectarse a la base de datos mediante *connect / as sysdba*.

Crear políticas para los recursos de plugins compatibles con NetApp

Antes de usar SnapCenter para realizar un backup de recursos específicos de un plugin compatible con NetApp, debe crear una política de backup para el recurso o el grupo de recursos que incluirá en el backup.

Antes de empezar

- Debe tener definida una estrategia de backup.

  Para obtener detalles, consulte la información sobre cómo definir una estrategia de protección de datos para los plugins compatibles con NetApp.

- 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 snapshots 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.
- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.
  - Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

La configuración principal de SnapLock se gestiona en la política de backup de SnapCenter y la configuración secundaria de SnapLock se gestiona mediante ONTAP.

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 sus detalles.
5. En la página Policy type, realice lo siguiente:
   a. Seleccione el tipo de almacenamiento.
   b. En la sección Custom backup settings, proporcione cualquier configuración de backup específica que tenga que pasarse al plugin en formato de clave-valor.

      Puede pasar varios pares de clave-valor al plugin.
6. En la página Snapshot and Replication, realice los siguientes pasos:
   a. 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.

   a. En la sección Configuración de instantánea, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionado en la página **Tipo de copia de seguridad**:

Si desea…	Realice lo siguiente…
Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino. El valor de retención máximo es 1018. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y especifique días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

b. Seleccione una etiqueta de política.

Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

7. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

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). Si la relación en ONTAP es del tipo Reflejo y almacén y solo se selecciona esta opción, Snapshot creado en el origen no se transferirá al destino, pero figurará en el destino. Si esta copia 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. Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Consulte "Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp en la página Topology".
Actualizar SnapVault después de crear una copia Snapshot local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP. Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el almacén de SnapLock, consulte Confirmar instantáneas en WORM en un destino de almacén. Consulte "Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp en la página Topology".

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 que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

8. 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 aplicación determinada. 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 izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione New Resource Group.
3. En la página Name, realice los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. Nota: 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	Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot. Por ejemplo, *customtext_resource group_policy_hostname o resource group_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la 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.

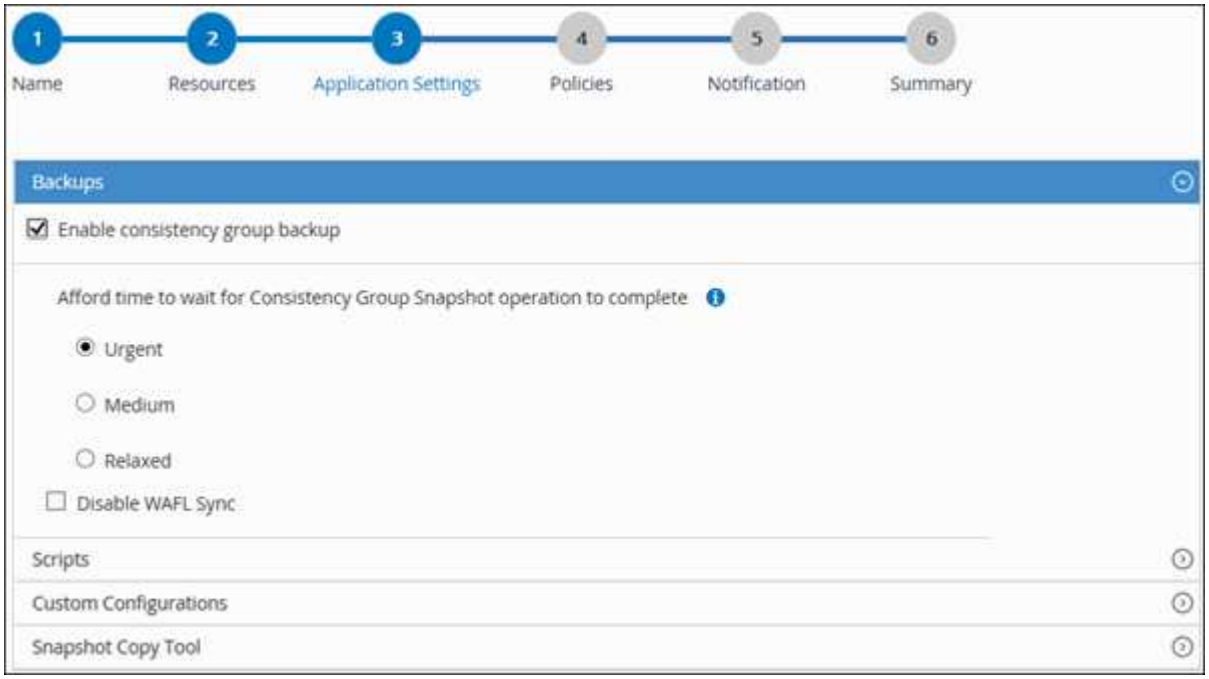
5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, seleccione la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. Opcional: En la página **Configuración de la aplicación**, haga lo siguiente:

   a. Seleccione 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 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.

+



   a. Seleccione la flecha Scripts y escriba los comandos previos y posteriores para el modo de inactividad, 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. Seleccione 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. 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. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.16151855 1942 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. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

c. Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

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 Snapshot. En el caso de recursos de Linux, esta opción no es aplicable.	Seleccione **SnapCenter with File System Consistency**. Esta opción no es aplicable para el plugin de SnapCenter para la base de datos SAP HANA.
SnapCenter creará una snapshot a 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 snapshots.	Seleccione **Otro** y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

7. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

      También puede crear una política seleccionando + .

      Las directivas se enumeran en la sección **Configurar horarios para directivas seleccionadas**.

   b. En la columna **Configure Schedules**, seleccione + para la directiva que desea configurar.

   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y seleccione OK.

      Donde 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.

8. En la lista desplegable **Preferencias de correo** de la página **Notificación**, selecciona los escenarios en los que deseas 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**.

9. Revisa el resumen y luego selecciona **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos en sistemas R2 de ASA

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.

- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:
   a. Escriba un nombre para el grupo de recursos en el campo Name.

      El nombre del grupo de recursos no debe superar los 250 caracteres.

   b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

      Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

   c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

   d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

      Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary Protection y debe realizar los siguientes pasos:
   a. Seleccione el tipo de política de replicación.

      No se admite la política de replicación síncrona.

   b. Especifique el sufijo del grupo de consistencia que desea utilizar.
   c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

      SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

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.

Antes de empezar

- 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 Core 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Realizar backup de los recursos de plugins compatibles con NetApp individuales

Si un recurso individual de plugins compatibles con NetApp 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.

Antes de empezar

- 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".

UI 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, filtre los recursos de la lista desplegable **View** 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 **Use custom name format for Snapshot copy** y, a continuación, introduzca un formato de nombre personalizado para el nombre de la instantánea.

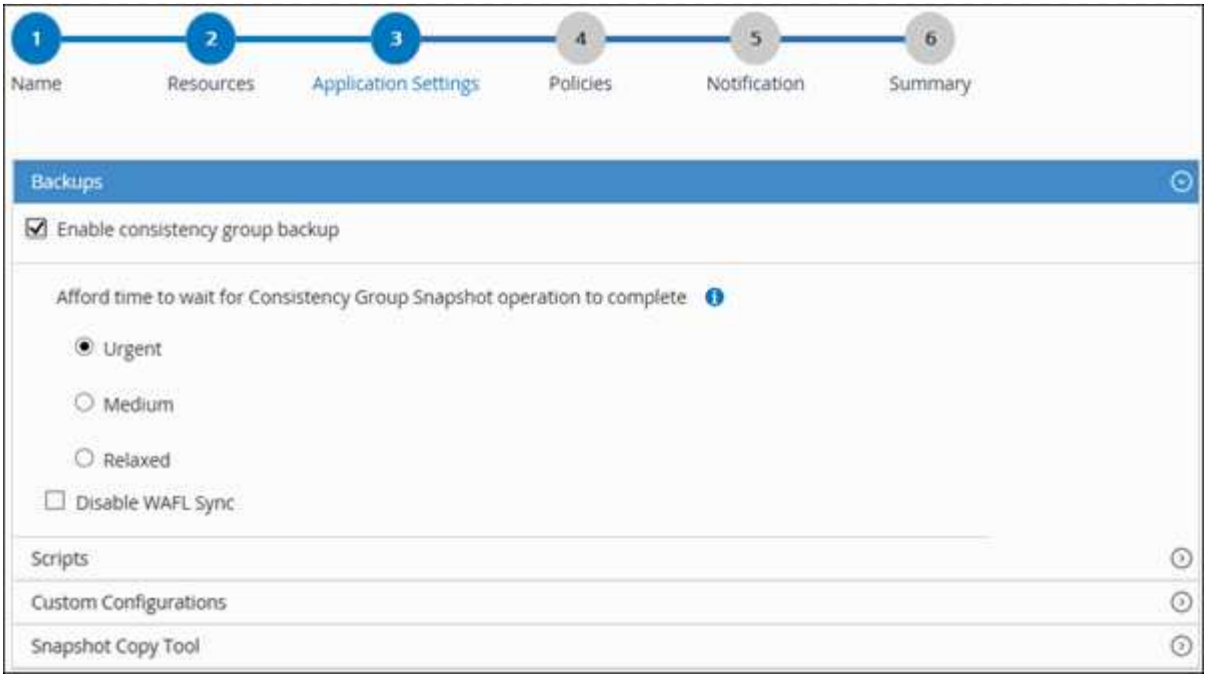
   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.
5. En la página Application Settings, realice lo siguiente:

   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 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.

+



a. Haga clic en la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación. 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 * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	Realice lo siguiente…
SnapCenter tomará una snapshot en el 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 Snapshot	Seleccione **SnapCenter with File System Consistency**.
Para escribir el comando para crear una snapshot	Seleccione **Otro** y luego ingrese el comando para crear una instantánea.

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 Configure Schedules correspondiente a la política para la cual se desea configurar una programación.

c. 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.

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. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

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

Se muestra la página de topología de los recursos.

9. Haga clic en **copia de seguridad ahora**.
10. 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**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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\
```

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 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.

   En este ejemplo, se crea una nueva política de backup:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin  -description 'testPolicy'
```

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_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

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:

```
Get-SmBackupReport -JobId 149

BackedUpObjects           : {QTREE2, QTREE}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 1
SmJobId                   : 149
StartDateTime             : 1/15/2024 1:35:17 AM
EndDateTime               : 1/15/2024 1:36:19 AM
Duration                  : 00:01:02.4265750
CreatedDateTime           : 1/15/2024 1:35:51 AM
Status                    : Completed
ProtectionGroupName       :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId       : 1
PolicyName                : test2
SmPolicyId                : 4
BackupName                :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DummyPlugin
PluginDisplayName         : DummyPlugin
JobTypeId                 :
JobHost                   : scc55.sccore.test.com
```

Realizar backup de grupos de recursos de plugins admitidos por NetApp

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.

Antes de empezar

- 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 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 seleccionado 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**.
   - 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`.

Supervise operaciones de backup de recursos de plugins compatibles con NetApp

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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 de los plugins compatibles con NetApp

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**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de copia de seguridad, haga clic en en el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**.

Se cancela la operación y el recurso se revierte al estado anterior.

Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp 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 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.

   Al hacer clic en el botón de actualización, se inicia una consulta del almacenamiento para ver un número preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Después de la copia de seguridad a petición, haciendo clic en el botón **Actualizar** actualiza los detalles de la copia de seguridad o clonación.

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.

7. Si desea eliminar un clon, selecciónelo en la tabla y haga clic en para eliminar el clon.

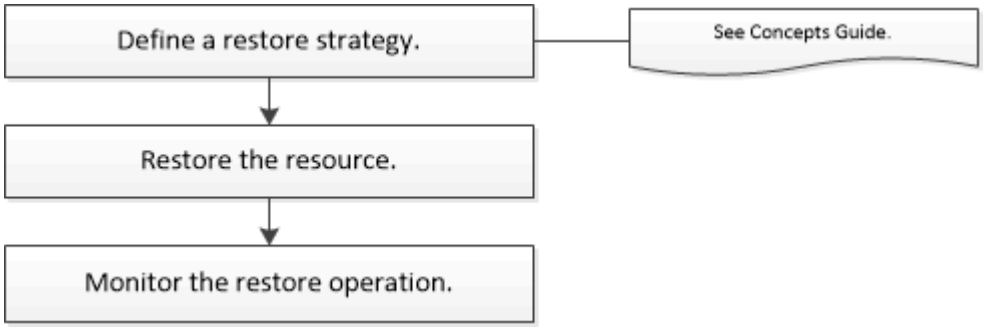
Restaurar recursos de plugins compatibles con NetApp

Restaurar recursos de plugins admitidos por NetApp

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.

Antes de empezar

- 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 Snapshots 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 NetApp compatible incluye dicha capacidad.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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, filtre los recursos de la lista desplegable **View** 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.

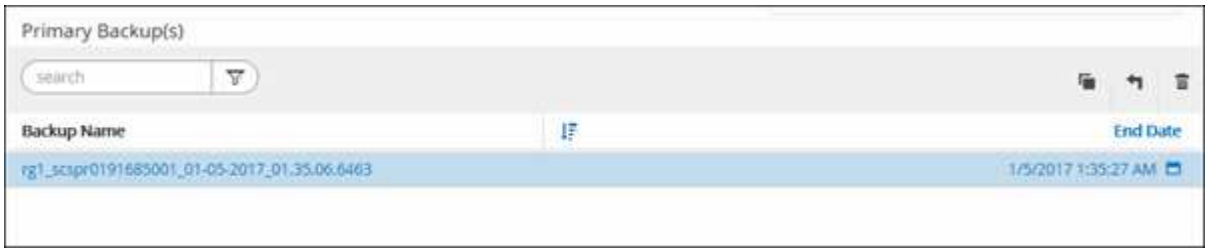
   Si el recurso no está protegido, se muestra *not protected* en la columna **Overall Status**.

   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.

3. 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.

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 seleccionó **Complete Resource**, se restaura la copia de seguridad del recurso.

      Si el recurso contiene volúmenes o qtrees como Storage Footprint, entonces los snapshots 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.
7. 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.

8. En la página **Post OPS**, escriba los comandos Mount y post restore que se ejecutarán después de realizar un trabajo de restauración.
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. SMTP también debe configurarse en la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

```
PS C:\> Open-Smconnection
```

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:

```
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. 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*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervise operaciones de restauración de recursos de plugins compatibles con NetApp

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.

Backups de recursos de plugins admitidos por Clone NetApp

Backups de recursos de plugins admitidos por Clone NetApp

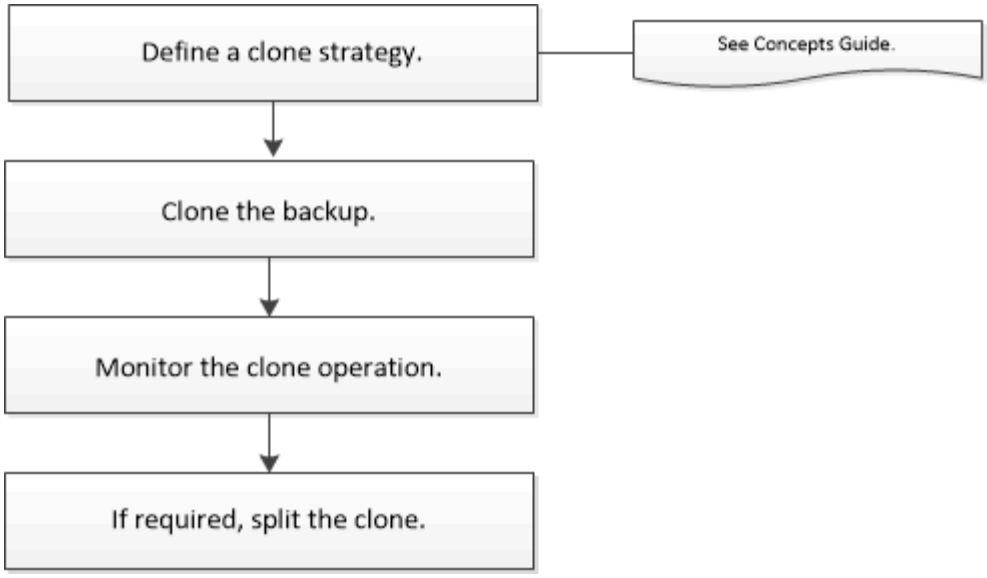
El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

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.

Antes de empezar

- 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 NetApp compatible 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).

Acerca de esta tarea

Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

UI 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 **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. 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. Escriba un sufijo que se anexará al nombre del recurso recién clonado. El sufijo garantiza que el recurso clonado sea único en el host. 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 previos o posteriores a la clonado que deben ejecutarse, respectivamente, antes o después de la operación de clonado. 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**.

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    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 operaciones de clonado de recursos de plugins admitidas por NetApp

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**.

Proteja los sistemas de archivos Unix

Tareas que pueden llevarse a cabo con el plugin de SnapCenter para sistemas de archivos Unix

Cuando el plugin para sistemas de archivos Unix está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar sistemas de archivos Unix. También es posible ejecutar tareas complementarias a estas operaciones.

- Detectar recursos
- Hacer backup de sistemas de archivos Unix
- 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

Configuraciones admitidas

Elemento	Configuración admitida
Entornos	• Servidor físico • Servidor virtual Almacenes de datos VVOL en NFS y SAN. El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Sistemas de ficheros	• SAN: ◦ Sistemas de archivos basados en LVM y no LVM ◦ LVM sobre VMDK ext3, ext4 y xfs • NFS: NFS v3, NFS v4.x
Protocolos	• FC • FCoE • ISCSI • NFS

Elemento	Configuración admitida
Multivía	sí

Limitaciones

- No se admite la combinación de RDM y discos virtuales en un grupo de volúmenes.
- No se admite la restauración de nivel de archivos.

  Sin embargo, puede realizar manualmente una restauración en el nivel de archivos clonando el backup y luego copiando los archivos manualmente.

- No se admite la combinación de sistemas de archivos distribuidos entre VMDK procedentes de NFS y almacenes de datos VMFS.
- No se admite NVMe.
- No se admite el aprovisionamiento.

Funciones

- 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.

- Automatiza las operaciones de backup, restauración y clonado para sistemas de archivos UNIX en el entorno de SnapCenter

Instale el plugin de SnapCenter para sistemas de archivos Unix

Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux

Antes de añadir un host e instalar el paquete de plugins para Linux, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Puede usar la autenticación basada en contraseña para el usuario raíz o no raíz, o para la autenticación basada en la clave SSH.

El complemento de SnapCenter para sistemas de archivos Unix puede ser instalado por un usuario que no sea root. 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 efectivo que no es raíz.

- Cree credenciales con modo de autenticación como Linux para el usuario de instalación.
- Debe haber instalado Java 11 en el host Linux.

> Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux.

Para obtener información sobre CÓMO descargar JAVA, consulte: "Descargas de Java para todos los sistemas operativos"

- Debe tener **bash** como shell por defecto para la instalación del plug-in.

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 • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM mínima para el plugin de SnapCenter en el host	2 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB 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	Java 11 Oracle Java y OpenJDK Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux. 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 la "Herramienta de matriz de interoperabilidad de NetApp" .

Añada hosts e instale el paquete de plugins para Linux 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. Los plugins se instalan automáticamente en hosts remotos.

- 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** como tipo de host.
Nombre de host	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. 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. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. 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 Seleccionar plugins para instalar, seleccione **Sistemas de archivos Unix**.
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. 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*. Opcionalmente, puede personalizar la ruta. Si utiliza la ruta personalizada, asegúrese de que el contenido predeterminado de los sudoers se actualiza con la ruta personalizada.
Omitir comprobaciones opcionales de preinstalación	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**.

   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*.

resultado

Todos los sistemas de archivos montados en el host se detectan automáticamente y se muestran en la página Resources. Si no aparece nada, haga clic en **Actualizar recursos**.

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 solo se enumeren las operaciones de instalación de 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 con el fin de interactuar con el servidor de SnapCenter. El servicio de cargador de plugins de SnapCenter se instala cuando se instala el paquete de plugins de SnapCenter para Linux.

Acerca de esta tarea

Después de instalar el paquete de plugins de SnapCenter para Linux, el servicio de cargador de plugins de SnapCenter se inicia automáticamente. 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. Los posibles valores son TRACE, DEBUG, INFO, WARN, ERROR, Y FATAL.
SPL_PROTOCOL	Muestra el protocolo que admite el cargador del plugin de SnapCenter. Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.

Nombre del parámetro	Descripción
SNAPCENTER_SERVER_PROTOCOL	Muestra el protocolo compatible con SnapCenter Server. 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. 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. 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. Puede agregar el valor si falta el valor predeterminado. 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*. 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. 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. 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. 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. 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 root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- Detenga el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
  - Como usuario no raíz, ejecute: `sudo /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:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Busque el estado del servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
  - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Busque el cambio en el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - Como usuario no raíz, ejecute: `sudo /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.

Antes de empezar

- 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*. Alternativamente, 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 su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM 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 sistemas de archivos Unix

Antes de ejecutar una operación de protección de datos, como un backup, un clon o una restauración, debe 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 utilizar el plugin para sistemas de archivos Unix, el administrador de SnapCenter debe instalar y configurar el servidor 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.

- Añada hosts, instale los plugins y detecte los recursos.
- Si va a utilizar SnapCenter Server para proteger sistemas de archivos Unix que residen en LUN o VMDK de VMware RDM, debe poner en marcha el plugin de SnapCenter para VMware vSphere y registrar el

plugin con SnapCenter.

- Instale Java en el host Linux.
- Configure SnapMirror y SnapVault en ONTAP si quiere realizar una replicación de backup.

Hacer backup de sistemas de archivos Unix

Descubra los sistemas de archivos UNIX disponibles para backup

Después de instalar el plugin, se detectan automáticamente todos los sistemas de archivos de ese host y se muestran en la página Resources. Puede añadir estos sistemas de archivos a grupos de recursos para realizar operaciones de protección de datos.

Antes de empezar

- Debe haber completado tareas, como instalar SnapCenter Server, añadir hosts y crear conexiones del sistema de almacenamiento.
- Si los sistemas de archivos residen en un disco de máquina virtual (VMDK) o una asignación de dispositivo sin formato (RDM), debe 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".

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 **Ruta** en la lista Ver.
3. Haga clic en **Actualizar recursos**.

   Los sistemas de archivos se muestran junto con cierta información, como el tipo, el nombre de host, las políticas y los grupos de recursos asociados, y el estado.

Crear directivas de backup para sistemas de archivos Unix

Antes de usar SnapCenter para realizar backups de sistemas de archivos Unix, debe crear una política de backup para el recurso o el 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. 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.

Antes de empezar

- En el marco de los preparativos para la protección de datos, completó tareas como instalar SnapCenter, añadir hosts, detectar sistemas de archivos y crear conexiones con el sistema de almacenamiento.
- Si desea replicar snapshots 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.

- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "Límites de objetos para la sincronización activa de SnapMirror".

Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.

    Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.

  Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

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 **Unix File Systems** de la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Name, escriba el nombre de la política y sus detalles.
6. En la página Backup and Replication, realice las siguientes acciones:
   a. Especifique la configuración de backup.
   b. Especifique la frecuencia de programación seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.
   c. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

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). Esta opción debe estar habilitada para la sincronización activa 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).
Número de reintentos con error	Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga.

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 and Replication:

Si desea…	Realice lo siguiente…
Mantenga un cierto número de Snapshots	Seleccione **Copias para guardar** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas. El valor de retención máximo es 1018. 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Retener copias para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de instantánea	Seleccione **Período de bloqueo de copia de instantánea** y especifique la duración en días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

8. Seleccione la etiqueta de política.

   Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

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 comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde la ruta _ /opt/NetApp/SnapCenter/scc/etc/allowed_commands.config_.

También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Cree grupos de recursos y adjunte políticas para sistemas de archivos Unix

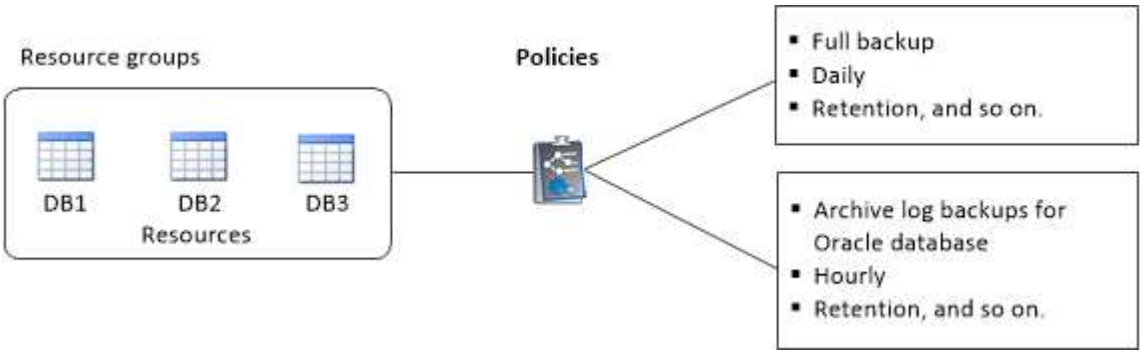
Un grupo de recursos es un contenedor donde se añaden recursos que se quieren proteger e incluir en un backup. El grupo de recursos permite realizar un backup con todos los datos que están asociados con los sistemas de archivos.

Acerca de esta tarea

- Una base de datos con archivos en grupos de discos de ASM debe tener el estado «MOUNT» o «OPEN» para verificar sus backups mediante la utilidad Oracle DBVERIFY.

  Añada 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:



- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admiten la adición de nuevos sistemas de archivos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de nuevos sistemas de archivos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

a. Escriba un nombre para el grupo de recursos en el campo Name.

> El nombre del grupo de recursos no debe superar los 250 caracteres.

b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque la casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

4. En la página Recursos, seleccione un nombre de host de sistemas de archivos Unix de 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.
6. En la página Application Settings, realice lo siguiente:
   - Seleccione la flecha Scripts y escriba los comandos previos y posteriores para el modo de inactividad, 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.
   - Seleccione una de las opciones de consistencia de backup:
     - Seleccione **Sistema de archivos consistente** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad y no se permiten operaciones de entrada o salida en el sistema de archivos durante la creación de la copia de seguridad.

> Para la consistencia del sistema de archivos, se tomarán snapshots de grupo de consistencia para las LUN involucradas en el grupo de volúmenes.

     - Seleccione **Consistente al bloqueo** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad.

> Si añadió diferentes sistemas de archivos en el grupo de recursos, todos los volúmenes de diferentes sistemas de archivos del grupo de recursos se colocarán en un grupo de consistencia.

7. 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 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**.

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.

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.

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

Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Unix en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

a. Escriba un nombre para el grupo de recursos en el campo Name.

> El nombre del grupo de recursos no debe superar los 250 caracteres.

b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

> Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos 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 ASA R2 de la sección Available Resources y muévalos a la sección Selected Resources.
6. En la página Application Settings, seleccione la opción de backup.
7. 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 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**.

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.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary

Protection y debe realizar los siguientes pasos:

a. Seleccione el tipo de política de replicación.

> No se admite la política de replicación síncrona.

b. Especifique el sufijo del grupo de consistencia que desea utilizar.

c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.

> SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.

> Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. 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.

2. 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.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Hacer backup de sistemas de archivos Unix

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, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Recursos, seleccione **Ruta** en la lista Ver.
3. Haga clic en y, a continuación, seleccione el nombre de host y los sistemas de archivos Unix para filtrar los recursos.
4. Seleccione el sistema de archivos del que desea realizar un backup.
5. En la página Resources, puede realizar los siguientes pasos:
   a. Marque la casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo: `customtext_policy_hostname` o. `resource_hostname`. De forma predeterminada, se añade una fecha/hora al nombre de Snapshot.

6. En la página Application Settings, realice lo siguiente:
   - Seleccione la flecha Scripts y escriba los comandos previos y posteriores para el modo de inactividad, 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.
   - Seleccione una de las opciones de consistencia de backup:
     - Seleccione **Sistema de archivos consistente** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad y no se realizan operaciones en el sistema de archivos durante la creación de la copia de seguridad.
     - Seleccione **Consistente al bloqueo** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad.
7. En la página Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.

      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 Configure Schedules para configurar una programación para la política que desea.
   c. En la ventana Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione `OK`.

policy_name es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

8. En la página Notificación, seleccione los escenarios en los que desea enviar los correos electrónicos desde la lista desplegable **Preferencias de correo electrónico**.

   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 el comando de PowerShell `Set-SmSmtpServer`.

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

   Se muestra la página de topología.

10. Haga clic en **copia de seguridad ahora**.
11. 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**.
12. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Realizar un backup de los grupos de recursos de sistemas de archivos Unix

Puede realizar una copia de seguridad de los sistemas de archivos Unix definidos en el grupo de recursos. Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si el grupo de recursos tiene una política anexada y una programación configurada, los backups se crean según esa programación.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. Escriba el nombre del grupo de recursos en el cuadro de búsqueda o haga clic en y seleccione la etiqueta.

   Haga clic en para cerrar el panel de filtros.

4. En la página Resource Group, seleccione el grupo de recursos que desea incluir en un backup.
5. En la página Backup, realice los siguientes pasos:
   a. Si tiene varias políticas asociadas con el grupo de recursos, seleccione la política de copia de seguridad que desea usar en la lista desplegable **Política**.

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 **copia de seguridad**.

6. Controla el progreso seleccionando **Monitor > Trabajos**.

Supervisar la copia de seguridad de sistemas de archivos Unix

Descubra cómo supervisar el progreso de las operaciones de backup y las operaciones de protección de datos.

Supervisar las operaciones de copia de seguridad de sistemas de archivos Unix

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 se muestra el estado del trabajo de copia de seguridad , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Vea los sistemas de archivos Unix protegidos en la página Topology

Al prepararse para realizar un backup, restaurar o clonar un recurso, puede ser útil ver una representación gráfica de todos los backups, sistemas de archivos restaurados y clones en el almacenamiento principal y secundario.

Acerca de esta tarea

En la página Topology, puede ver todos los backups, los sistemas de archivos restaurados y los clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups, sistemas de archivos restaurados 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.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

- El sitio de réplica está activo.
- El sitio de réplica está inactivo.
- No se restableció la relación de reflejo o almacén secundario.
- 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.

     Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

     Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

     Cuando el sistema de archivos se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock del backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

     Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

     - Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.
     - Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya

creado una copia de seguridad.

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 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.

7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Ejemplo que muestra backups y clones en el almacenamiento principal

Restaurar y recuperar sistemas de archivos Unix

Restaurar sistemas de archivos Unix

En caso de pérdida de datos, puede utilizar SnapCenter para restaurar sistemas de archivos Unix.

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 sobre los parámetros que se pueden utilizar con el comando y sus descripciones se pueden obtener ejecutando Get-Help *command_name*. Alternativamente, también puede consultar la "Guía de referencia de comandos del software SnapCenter" .

- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.

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 **Ruta** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione el sistema de archivos en la vista de detalles o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología.

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:
   - Para los sistemas de archivos NFS, por defecto se selecciona la opción **Connect and Copy** restore. También puede seleccionar **Reversión de volumen** o **Restauración rápida**.
   - Para sistemas de archivos que no son NFS, el alcance de la restauración se selecciona según el diseño.

     Es posible que los nuevos archivos creados después de la copia de seguridad no estén disponibles después de la restauración, según el tipo y el diseño del sistema de archivos.
7. En la página PreOps, escriba los comandos previos a la restauración que se ejecutarán antes de realizar un trabajo de restauración.
8. En la página PostOps, escriba los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ubicación */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config* path.

9. 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.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Si la operación de restauración falla, no se admite la reversión.

En caso de restauración de un sistema de archivos que reside en el grupo de volúmenes, el contenido antiguo del sistema de archivos no se eliminará. Solo el contenido del sistema de archivos clonado se copiará al sistema de archivos de origen. Esto es aplicable cuando hay varios sistemas de archivos en el grupo de volúmenes y restauraciones predeterminadas del sistema de archivos NFS.

11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Supervisar las operaciones de restauración de sistemas de archivos Unix

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.

Clonar sistemas de archivos Unix

Clonar backup de sistema de archivos Unix

Puede utilizar SnapCenter para clonar el sistema de archivos Unix mediante la copia de seguridad del sistema de archivos.

Antes de empezar

- Para omitir la actualización del archivo fstab, debe configurarse el valor de *SKIP_FSTAB_UPDATE* como **true** en el archivo *agent.properties* ubicado en */opt/NetApp/snapcenter/scc/etc*.
- Puede contar con un nombre de volumen de clon estático y una ruta de unión si se configura el valor de *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* a **true** en el archivo *agent.properties* ubicado en */opt/NetApp/snapcenter/scc/etc*. Después de actualizar el archivo, debe reiniciar el servicio creador del complemento SnapCenter ejecutando el comando: `/opt/NetApp/snapcenter/scc/bin/scc restart`.

  Ejemplo: Sin esta propiedad, el nombre del volumen clonado y la ruta de unión serán como <Source_volume_name>_Clone_<Timestamp>, pero ahora serán <Source_volume_name>_Clone_<Clone_Name>

  Esto mantiene el nombre constante para que pueda mantener el archivo fstab actualizado manualmente si no prefiere actualizar el fstab por 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, seleccione **Ruta** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione el sistema de archivos en la vista de detalles o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología.

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 Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el servidor	De forma predeterminada, se llena el host de origen.
Clone el punto de montaje	Especifique la ruta de acceso en la que se montará el sistema de archivos.

7. En la página Scripts, realice los siguientes pasos:

a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.

> Debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ruta */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*.

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 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.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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 operaciones de división de volúmenes de FlexClone, consulte, "Divida un volumen FlexClone de su volumen principal".
- 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.

Opción	Descripción
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 **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o 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.

Información relacionada

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

Supervisar operaciones de clonación de sistemas de archivos Unix

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**.

Proteja las aplicaciones que se ejecutan en Azure NetApp Files

Proteja las aplicaciones que se ejecutan en Azure NetApp Files

SnapCenter admite la protección de aplicaciones como Oracle, SQL y SAP HANA que residen en Azure NetApp Files. A partir de la versión 6.0.1, SnapCenter admite la función de backup de Azure NetApp Files que amplía las funcionalidades de protección de datos de Azure NetApp Files al proporcionar una solución de backup totalmente gestionada para la recuperación, el archivado y el cumplimiento de normativas a largo plazo.

Azure NetApp Files es una solución de almacenamiento premium que puede ser costosa para la retención de backup a largo plazo. Para optimizar los costes, puede mover los backups desde el almacenamiento de Azure NetApp Files a un almacén de objetos de Azure. A partir de SnapCenter 6,0.1, puede realizar backups y clonar aplicaciones que residen en Azure NetApp Files en Azure Blob Storage (almacén de objetos). Puede conservar dos copias de sus datos, copias snapshot de volúmenes en almacenamiento de Azure NetApp Files para recuperación a corto plazo y otra copia en Azure Blob Storage para recuperación a largo plazo.

Cuando se habilita una política con el backup de Azure NetApp Files y se asocia con un recurso, SnapCenter gestiona la creación de copias Snapshot de volúmenes y el backup de ellas en Azure Blob Storage. SnapCenter crea el almacén de backup y habilita el backup del volumen. Si habilitó el backup para el volumen, SnapCenter utiliza el almacén existente.

Limitaciones

- No se admiten las funcionalidades de almacenamiento de objetos para los sistemas de almacenamiento FAS, ASA o AFF ONTAP y Amazon FSx para NetApp ONTAP.
- Los flujos de trabajo de montaje y catálogo de Oracle y SAP HANA no son compatibles con los backups de almacenamiento de objetos, pero sí con las copias Snapshot.
- No se admiten los clones de Oracle PDB para los backups de almacenamiento de objetos, pero sí para las Snapshot.
- No se admite la verificación de backups en el almacenamiento de objetos, la compatibilidad con API DE REST, la gestión del ciclo de vida de clones desde el almacenamiento de objetos e las funciones de generación de informes para los backups de almacenamiento de objetos.
- No se admite la restauración desde backups en Azure Blob Storage a Azure NetApp Files. También puede usar la opción clone.
- No se admite la división de clones.

Instale SnapCenter y cree las credenciales

Instalar SnapCenter en la máquina virtual de Azure

Puede descargar el software SnapCenter del sitio de soporte de NetApp e instalar el software en la máquina virtual de Azure.

Antes de empezar

- Asegúrese de que la máquina virtual de Azure Windows cumple los requisitos de instalación del servidor SnapCenter. Para obtener más información, consulte "Requisitos para instalar el servidor SnapCenter".
- Si es nuevo en Azure NetApp Files y no tiene una cuenta de NetApp existente, asegúrese de que se ha registrado para poder acceder al software de SnapCenter. Para obtener más información, consulte "Regístrese para acceder al software de SnapCenter".

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 se cumplen los correctos, se muestran mensajes de error o 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 “%” no está soportado en la ruta de acceso personalizada de la base de datos del repositorio. Si incluye “%” 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.

Registre el producto para habilitar la asistencia

Si es nuevo en NetApp y no tiene una cuenta de NetApp existente, debe registrar el producto para habilitar el soporte.

Pasos

1. Después de instalar SnapCenter, vaya a **Ayuda > Acerca de**.
2. En el cuadro de diálogo *About SnapCenter*, anote la instancia de SnapCenter, un número de 20 dígitos que comienza por 971.
3. Haga clic en https://register.netapp.com.
4. Haga clic en **no soy un cliente registrado de NetApp**.
5. Especifique sus datos para registrarse.
6. Deje en blanco el campo Número de serie de referencia de NetApp.

7. Seleccione **SnapCenter** en la lista desplegable Línea de productos.
8. Seleccione el proveedor de facturación.
9. Introduzca el identificador de instancia de SnapCenter de 20 dígitos.
10. Haga clic en **Enviar**.

Cree las credenciales de Azure en SnapCenter

Debe crear la credencial de Azure en SnapCenter para acceder a la cuenta de Azure NetApp.

Antes de empezar

- Asegúrese de haber creado el principal de servicio en Azure.
- Asegúrese de que tiene disponibles el ID de inquilino, el ID de cliente y la clave secreta asociada al principal de servicio.
  - El ID de inquilino se puede encontrar en Azure Portal en la página Visión General de Entra ID.
  - El ID de cliente también se conoce como ID de aplicación para Enterprise App/Service Principal. Esto se puede encontrar en el portal de Azure en la página Visión general de la aplicación empresarial que ha creado para actuar como principal de servicios para SnapCenter.
  - La clave secreta de cliente también se conoce como valor secreto. Puede crear este secreto de cliente en Azure Portal navegando a **Registros de aplicaciones** bajo Entra ID. Después de seleccionar la aplicación empresarial que creó, navegue a **Certificados y secretos** y luego a **Nuevo secreto de cliente**.

    Solo se puede acceder al valor secreto cuando se crea. No podrá acceder a él más tarde.

  - Se deben otorgar permisos al principal de servicio. La función de Contributor permitirá al director de servicio realizar las acciones necesarias en Azure. Esto se puede otorgar desde la página Control de Acceso (IAM) de la página Suscripción.

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, especifique la siguiente información necesaria para crear la credencial.

Para este campo…	Realice lo siguiente…
Nombre de credencial	Escriba un nombre para la credencial.
Modo de autenticación	Seleccione **Azure Credential** de la lista desplegable.
ID de inquilino	Introduzca el ID de inquilino.
ID del cliente	Introduzca el ID de cliente.

Para este campo…	Realice lo siguiente…
Clave secreta de cliente	Introduzca la clave secreta del cliente.

5. Haga clic en **Aceptar**.

Configure la cuenta de almacenamiento de Azure

Debe configurar la cuenta de almacenamiento de Azure en SnapCenter.

La cuenta de almacenamiento de Azure contiene detalles sobre el ID de suscripción, las credenciales de Azure y la cuenta de Azure NetApp.

Las licencias estándar y basadas en capacidad no son requeridas para Azure NetApp Files.

Pasos

1. En el panel de navegación izquierdo, haga clic en **sistemas de almacenamiento**.
2. En la página Sistemas de almacenamiento, seleccione **Azure NetApp Files** y haga clic en **Nuevo**.
3. Seleccione la credencial, el ID de suscripción y la cuenta de NetApp en las listas desplegables correspondientes.
4. Haga clic en **Enviar**.

Cree la credencial para añadir el host del plugin

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.

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, especifique la siguiente información necesaria para crear la credencial.

Para este campo…	Realice lo siguiente…
Nombre de credencial	Escriba un nombre para la credencial.
Modo de autenticación	Seleccione el modo de autenticación de la lista desplegable.
Tipo de autenticación	Seleccione **Basado en contraseña** o **Basado en clave SSH** (solo para host Linux).
Nombre de usuario	Especifique el nombre de usuario.

Para este campo…	Realice lo siguiente…
Contraseña	Si seleccionó autenticación basada en contraseña, especifique la contraseña.
Clave privada SSH	Si seleccionó la autenticación basada en clave SSH, especifique la clave privada.
Use privilegios sudo	Seleccione la casilla de comprobación Use sudo privileges si va a crear credenciales para usuarios que no son raíz. Esto solo se aplica a usuarios Linux.

5. Haga clic en **Aceptar**.

Proteger las bases de datos SAP HANA

Añadir hosts e instalar el plugin de SnapCenter para base de datos SAP HANA

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.

Antes de empezar

- 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.
- Si está instalando en el host centralizado, asegúrese de que el software cliente SAP HANA esté instalado en ese host y abra los puertos necesarios en el host de la base de datos SAP HANA para ejecutar las consultas SQL HDB de forma remota.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Verifique que la pestaña **Managed Hosts** esté seleccionada.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:
   a. En el campo Tipo de host, seleccione el tipo de host.
   b. En el campo Host name, introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.
   c. En el campo Credenciales, introduzca la credencial que ha creado.
5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Haga clic en **Enviar**.

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.

9. Supervise el progreso de la instalación.

Añada una base de datos SAP HANA

Debe añadir manualmente la base de datos SAP HANA.

Acerca de esta tarea

Los recursos se deben añadir manualmente si el plugin está instalado en un servidor centralizado. Si el plugin de SAP HANA se instala en el host de la base de datos de HANA, el sistema HANA se detecta de forma automática.

La detección automática no es compatible con la configuración de varios hosts HANA. Solo es necesario añadir a través del plugin centralizado.

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 Resources, haga clic en **Add SAP HANA Database**.
3. En la página Provide Resource Details, realice las siguientes acciones:
   a. Introduzca el tipo de recurso como Single Container, Multitenant Database Container o Non-data Volume.
   b. Introduzca el nombre del sistema SAP HANA.
   c. Introduzca el ID del sistema (SID).
   d. Seleccione el host del plugin.
   e. Introduzca la clave para conectarse al sistema SAP HANA.
   f. Introduzca el nombre de usuario para el que se configuró la clave de almacenamiento de usuario seguro HDB.
4. En la página Proporcionar espacio de almacenamiento, seleccione **Azure NetApp Files** como tipo de almacenamiento.
   a. Seleccione la cuenta de Azure NetApp.
   b. Seleccione el pool de capacidad y los volúmenes asociados.
   c. Haga clic en **Guardar**.
5. Revise el resumen y, a continuación, haga clic en **Finalizar**.

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.

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 Policy type, realice los siguientes pasos:
   a. Seleccione **Azure NetApp Files** como tipo de almacenamiento.
   b. Seleccione **Basado en archivos** si desea realizar una comprobación de integridad de la base de datos.
   c. Seleccione **Basado en Snapshot** si desea crear una copia de seguridad utilizando la tecnología Snapshot.
6. En la página Snapshot and backup, realice los siguientes pasos:
   a. Seleccione la frecuencia del backup programado.
   b. Especifique la configuración de retención.
   c. Si desea habilitar la copia de seguridad de Azure NetApp Files, seleccione **Habilitar copia de seguridad** y especifique la configuración de retención.
7. Revise el resumen y haga clic en **Finalizar**.

Cree grupos de recursos y conecte políticas de backup de SAP HANA

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 Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.
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 Snapshot.

4. En la página Resources, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

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 Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.
   b. En la columna Configure Schedules, haga clic en + en la política 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**.
7. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
8. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Realizar un backup de las bases de datos SAP HANA que se ejecutan en Azure NetApp Files

Si un recurso aún 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 izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.
3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.
5. En la página Application Settings, realice lo siguiente:
   a. Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales.
   b. Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.
   c. Seleccione la flecha **Configuraciones personalizadas** y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
   d. Seleccione la **Herramienta de copia de instantáneas > SnapCenter sin consistencia del sistema de archivos** para crear instantáneas.

      La opción **File System Consistency** solo se aplica a las aplicaciones que se ejecutan en hosts de Windows.
6. En la página Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.
   b. Seleccione + en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.
   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

      policy_name es el nombre de la directiva seleccionada.

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. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

8. Revisa el resumen y luego selecciona **Finalizar**.
9. Seleccione **Back up Now**.
10. En la página Backup, realice los siguientes pasos:
    a. Si hay varias políticas asociadas con el recurso, 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.

11. Seleccione **copia de seguridad**.
12. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Realice un backup de grupos de recursos SAP HANA

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.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
    a. Si hay varias políticas asociadas con el 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. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Restaurar y recuperar bases de datos SAP HANA

Es posible restaurar y recuperar datos de los backups.

Acerca de esta tarea

Para los sistemas Auto Discovered HANA, si se selecciona la opción **Complete Resource**, la restauración se realiza utilizando la tecnología Single File snapshot restore. Si la casilla de verificación **Fast Restore** está seleccionada, se utiliza la tecnología Volume Revert.

Para los recursos agregados manualmente, siempre se utiliza la tecnología Volume Revert.

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, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.
3. Seleccione el recurso, o bien seleccione un grupo de recursos y, a continuación, elija un recurso de ese grupo.
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**.

   Se restauran todos los volúmenes de datos configurados de la base de datos SAP HANA.

7. Para los sistemas HANA detectados automáticamente, en la página Restore Scope, realice las siguientes acciones:
   a. Seleccione **Recuperar al estado más reciente** si desea recuperarse lo más cerca posible de la hora actual.
   b. Seleccione **Recuperar a punto en el tiempo** si desea recuperar al punto en el tiempo especificado.
   c. Seleccione **Recuperar a copia de seguridad de datos especificada** si desea recuperar una copia de seguridad de datos específica.
   d. Seleccione **No recovery** si no desea recuperar ahora.
   e. Especifique la ubicación de backup de registros.
   f. Especifique la ubicación del catálogo de backups.
8. 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.
9. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.
10. 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 la página **Ajustes** > **Ajustes globales**.

11. Revise el resumen y, a continuación, haga clic en **Finalizar**.
12. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Clone el backup de base de datos SAP HANA

Puede utilizar SnapCenter para clonar una base de datos SAP HANA con el backup de esa base de datos. Los clones creados son clones gruesos y se crean en el pool de capacidad primario.

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, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.
3. Seleccione el recurso o el grupo de recursos.
4. En la vista Administrar copias, seleccione **Copias de seguridad** en el sistema de almacenamiento primario.
5. Seleccione el backup de datos de la tabla y haga clic en .
6. En la página Location, lleve a cabo las siguientes acciones:

    a. Seleccione el host que tiene el plugin SAP HANA instalado para gestionar el sistema HANA clonado.

    Puede ser un host de plugin centralizado o un host de sistema HANA.

    > Si el plugin de HANA se instala en un host centralizado que gestiona bases de datos de HANA en otros hosts, mientras crea o elimina clones, SnapCenter omite intencionalmente las operaciones del lado del host (montar o desmontar sistema de archivos) como servidor de destino es un host centralizado. Es necesario utilizar scripts previos o posteriores a la clonado para realizar las operaciones de montaje y desmontaje.

    a. Introduzca el SID de SAP HANA para clonar a partir de los backups existentes.
    b. Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados.
    c. Si los volúmenes de ANF de base de datos SAP HANA están configurados en un pool de CAPACIDAD DE CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

    Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

7. En la página Scripts, realice los siguientes pasos:

    a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.
    b. Escriba el comando de montaje para montar un sistema de archivos en un host.

    Si se detecta automáticamente el sistema HANA de origen y se instala el plugin del host de destino del clon en el host SAP HANA, SnapCenter desmonta automáticamente los volúmenes de datos de HANA existentes en el host de destino del clonado y monta los volúmenes de datos de HANA recién clonados.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

> La división de clones está deshabilitada para los clones de ANF porque el clon de ANF ya es un volumen independiente creado a partir de la snapshot seleccionada.

Proteger bases de datos de Microsoft SQL Server

Añadir hosts e instalar el plugin de SnapCenter para base de datos de SQL Server

SnapCenter admite la protección de datos de instancias de SQL en recursos compartidos de SMB en Azure NetApp Files. Se admiten las configuraciones de grupos de disponibilidad (AG) independientes.

Debe usar la página SnapCenter Add Host para añadir hosts y, a continuación, instalar el paquete de los plugins. Los plugins se instalan automáticamente en hosts remotos.

Antes de empezar

- 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.

Pasos

1. En el panel de navegación izquierdo, seleccione **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página hosts, haga lo siguiente:
   a. En el campo Tipo de host, seleccione el tipo de host.
   b. En el campo Host name, introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.
   c. En el campo Credenciales, introduzca la credencial que ha creado.
5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Seleccione **Enviar**.
8. Seleccione **Configurar directorio de registro** y en la página Configurar directorio de registro de host, introduzca la ruta SMB del directorio de registro de host y haga clic en **Guardar**.
9. Haga clic en **Enviar** y supervise el progreso de la instalación.

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.

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 Policy type, realice los siguientes pasos:
    a. Seleccione **Azure NetApp Files** como tipo de almacenamiento.
    b. Seleccione el tipo de backup.
        i. Seleccione **Full Backup and Log Backup** si desea realizar una copia de seguridad de los archivos de la base de datos y los registros de transacciones.
        ii. Seleccione **Full Backup** si desea realizar una copia de seguridad solo de los archivos de la base de datos.
        iii. Seleccione **Log Backup** si desea realizar una copia de seguridad solo de los registros de transacciones.
        iv. Seleccione **Copia de seguridad de solo copia** si desea realizar una copia de seguridad de sus recursos utilizando otra aplicación.
    c. En la sección Availability Group Settings, realice las siguientes acciones:
        i. Seleccione Backup on preferred backup replica si desea realizar un backup solo en la réplica.
        ii. Seleccione la réplica principal o secundaria del AG para el backup.
        iii. Seleccione la prioridad de backup.
6. En la página Snapshot and backup, realice los siguientes pasos:
    a. Seleccione la frecuencia del backup programado.
    b. Especifique la configuración de retención según el tipo de backup seleccionado.
    c. Si desea habilitar la copia de seguridad de Azure NetApp Files, seleccione **Habilitar copia de seguridad** y especifique la configuración de retención.
7. En la página Verification, realice los siguientes pasos:
    a. En la sección Run verification for following backup schedules, seleccione la frecuencia de backup.
    b. En la sección Database consistency check options, realice las siguientes acciones:
        i. 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.
        ii. Seleccione **Suprimir todos los mensajes informativos (NO INFOMSGS)** para suprimir todos los mensajes informativos.

            Seleccionado de forma predeterminada.

        iii. Seleccione **Display all reported error messages per object (ALL_ERRORMSGS)** para visualizar todos los errores notificados por objeto.
        iv. 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.

        v. Seleccione **Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una copia Snapshot interna de la base de datos (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una instantánea 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.

8. Revise el resumen y haga clic en **Finalizar**.

Cree grupos de recursos y asocie las políticas de backup de SQL

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 Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.
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 Snapshot.

4. En la página Resources, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.
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 Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.
   b. En la columna Configure Schedules, haga clic en en la política 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**.
   d. Seleccione Microsoft SQL Server Scheduler.
7. En la página Verification, realice los siguientes pasos:

a. Seleccione el servidor de verificación.

b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en * *.

c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.

d. Haga clic en **Aceptar**.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Realizar backups de bases de datos de SQL Server que se ejecutan en Azure NetApp Files

Si un recurso aún no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

Antes de empezar

Debe crear un balanceador de carga si el clúster de conmutación por error de Azure Windows no tiene una IP de clúster asignada o si no es accesible desde SnapCenter. La IP del equilibrador de carga se debe configurar y es posible acceder a ella desde el servidor de SnapCenter.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos**, **Instancia** o **Grupo de disponibilidad** en la lista desplegable Ver.
3. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.
4. En la página Policies, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.

b. Seleccione en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

policy_name es el nombre de la directiva seleccionada.

d. Seleccione **Use Microsoft SQL Server scheduler** y, a continuación, seleccione la instancia del programador en la lista desplegable **Scheduler Instance** que está asociada con la política de programación.

5. En la página Verification, realice los siguientes pasos:

a. Seleccione el servidor de verificación.

b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en * *.

c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.

d. Haga clic en Aceptar.

6. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
7. Revise el resumen y, a continuación, haga clic en **Finalizar**.
8. Seleccione **Back up Now**.
9. En la página Backup, realice los siguientes pasos:
   a. Si hay varias políticas asociadas con el recurso, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
   b. Seleccione **Verificar después de la copia de seguridad**.
   c. Seleccione **copia de seguridad**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Realizar un backup de grupos de recursos de SQL Server

Puede realizar el backup de los grupos de recursos que consten de varios recursos. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
   a. Si hay varias políticas asociadas con el grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
   b. Después de la copia de seguridad, seleccione **Verify** para verificar la copia de seguridad bajo demanda.
   c. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Restaurar y recuperar bases de datos de SQL Server

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server. La restauración de una base de datos es un proceso multifásico que copia todos los datos y las páginas de registro de una copia de seguridad específica de SQL Server a una base de datos específica.

Antes de empezar

- Configure la instancia de destino con un usuario de Active Directory que pertenezca al dominio de Active Directory de SMB AD y tenga permisos para establecer los permisos de archivo adecuadamente.

- Configure las credenciales a nivel de instancia de SnapCenter .
- Si la base de datos SQL existe en un recurso compartido CIFS, entonces la cuenta RunAS y la cuenta de servicio SQL (cuenta de dominio) del host del complemento deben formar parte de `BUILTIN\Administrators` grupo del servidor CIFS en ONTAP.
- Las configuraciones SMB no admiten la autenticación SQL para la instancia de destino. Configure la instancia de destino en SnapCenter con un usuario de Active Directory que tenga los permisos necesarios.
- Si la cuenta de servicio del complemento SnapCenter no es un usuario de Active Directory, asegúrese de que haya disponible un usuario con control total sobre los volúmenes de origen al restaurar en un host alternativo.

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.
4. En la vista Administrar copias, seleccione **Copias de seguridad** del 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:
   a. Seleccione **Restaurar la base de datos en el mismo host donde se creó la copia de seguridad** para restaurar la base de datos en el mismo servidor SQL.
   b. Seleccione **Restaurar la base de datos en un host alternativo** si desea restaurar la base de datos en un servidor SQL diferente en el mismo host o en otro donde se realizan las copias de seguridad.
7. En la página Restore Scope, seleccione una de las siguientes opciones:
   a. Seleccione **Ninguno** cuando necesite restaurar sólo la copia de seguridad completa sin ningún registro.
   b. 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.
   c. 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.
   d. 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.
   e. 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.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el proceso de restauración mediante la página **Monitor** > **Jobs**.

Clone el backup de base de datos de SQL Server

Es posible utilizar SnapCenter para clonar una base de datos de SQL con el backup de esa base de datos. Los clones creados son clones gruesos y se crean en el pool de capacidad primario.

Acerca de esta tarea

Debe asegurarse de que la instancia de destino para el clon esté configurada con un usuario de Active Directory que pertenezca al dominio de directorio SMB ADactive y que tenga permisos para establecer los permisos de archivo adecuadamente. Debe configurar las credenciales en SnapCenter a nivel de instancia.

La autenticación SQL para la instancia de destino no se admitirá para las configuraciones SMB. La instancia de destino se debe configurar en SnapCenter con el usuario de Active Directory que tenga los permisos necesarios.

Si la cuenta de servicio de servicios del plugin de SnapCenter no es un usuario de directorio activo, se requiere el usuario con control total sobre los volúmenes de origen para poder suplantar la trama y realizar la operación requerida.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos o el grupo de recursos.
4. En la página de vista **Administrar copias**, seleccione la copia de seguridad desde el sistema de almacenamiento primario.
5. Seleccione el backup y, a continuación, seleccione .
6. En la página **Clonar opciones**, proporcione todos los detalles requeridos.
7. En la página ubicación, seleccione una ubicación de almacenamiento para crear un clon.

   Si los volúmenes de ANF de bases de datos de SQL Server se configuran en un pool de CAPACIDAD DE CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

   Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

8. En la página Logs, seleccione una de las siguientes opciones:
   a. Seleccione **Ninguno** si desea clonar solo la copia de seguridad completa sin ningún registro.
   b. Seleccione **All log backups** si desea clonar todas las copias de seguridad de registros disponibles con fecha posterior a la copia de seguridad completa.
   c. Seleccione **by log backups until** si desea clonar la base de datos en función de los registros de copia de seguridad que se crearon hasta el registro de copia de seguridad con la fecha seleccionada.
   d. Seleccione **Por fecha específica hasta** si no desea aplicar los registros de transacciones después de la fecha y hora especificadas.
9. En la página **Script**, introduzca el tiempo de espera del script, la ruta y los argumentos del script previo o script posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente.

10. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revisa el resumen y luego selecciona **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

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.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos o el grupo de recursos.
4. En la página de vista **Administrar copias**, seleccione la copia de seguridad desde el sistema de almacenamiento primario.
5. Seleccione el backup y, a continuación, seleccione .
6. En la página **Clonar opciones**, proporcione todos los detalles requeridos.
7. En la página ubicación, seleccione una ubicación de almacenamiento para crear un clon.

   Si los volúmenes de ANF de bases de datos de SQL Server se configuran en un pool de CAPACIDAD DE CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

   Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.
8. En la página **Script**, introduzca el tiempo de espera del script, la ruta y los argumentos del script previo o script posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente.
9. En la página Schedule, realice una de las siguientes acciones:
   - Seleccione **Ejecutar ahora** si desea ejecutar el trabajo de clonado inmediatamente.
   - Seleccione **Configure schedule** cuando desee determinar con qué frecuencia debe producirse la operación de clonación, cuándo debe iniciarse la programación de clonación, en qué día debe producirse la operación de clonación, cuándo debe caducar la programación y si los clones deben eliminarse después de que caduque la programación.
10. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revisa el resumen y luego selecciona **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Proteger bases de datos de Oracle

Añadir hosts e instalar el plugin de SnapCenter para base de datos de Oracle

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.

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.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Verifique que la pestaña **Managed Hosts** esté seleccionada.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:
   a. En el campo Tipo de host, seleccione el tipo de host.
   b. En el campo Host name, introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.
   c. En el campo Credenciales, introduzca la credencial que ha creado.
5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Haga clic en **Enviar**.
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.

9. Supervise el progreso de la instalación.

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.

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 Policy type, realice los siguientes pasos:
   a. Seleccione **Azure NetApp Files** como tipo de almacenamiento.
   b. Seleccione el tipo de backup como backup online o sin conexión.
   c. Si desea catalogar la copia de seguridad con Oracle Recovery Manager (RMAN), seleccione **Catalog**

backup with Oracle Recovery Manager (RMAN).

d. Si desea reducir los registros de archivos después de la copia de seguridad, seleccione **Prune archive logs after backup**.

e. Especifique la configuración de eliminación de archive log.

7. En la página Snapshot and backup, realice los siguientes pasos:

a. Seleccione la frecuencia del backup programado.

b. Especifique la configuración de retención.

c. Si desea habilitar la copia de seguridad de Azure NetApp Files, seleccione **Habilitar copia de seguridad** y especifique la configuración de retención.

8. 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.

9. En la página Verification, seleccione la programación de backup para la que desea realizar la operación de verificación e introduzca la ruta y los argumentos del script previo o posterior que desea ejecutar antes o después de la operación de verificación, según corresponda.

10. Revise el resumen y haga clic en **Finalizar**.

Crear grupos de recursos y asociar las políticas de backup 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. 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 Resources, haga clic en **New Resource Group**.

3. En la página Name, realice los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.
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 Snapshot.
Destino del archivo archive log	Especifique los destinos de los archivos de registro de archivos.

4. En la página Resources, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.
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 Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.
   b. En la columna Configure Schedules, haga clic en + en la política 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**.
7. En la página Verification, realice los siguientes pasos:
   a. Seleccione el servidor de verificación.
   b. Seleccione la política para la que desea configurar el programa de verificación y haga clic en * + .
   c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.
   d. Haga clic en **Aceptar**.
8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Realizar backups de las bases de datos de Oracle que se ejecutan en Azure NetApp Files

Si un recurso aún 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 izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** en la lista desplegable Ver.
3. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.
4. En la página Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.
   b. Seleccione + en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.
   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.
5. En la página Verification, realice los siguientes pasos:
   a. Seleccione el servidor de verificación.
   b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en + *

*.

c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.

d. Haga clic en Aceptar.

6. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
7. Revise el resumen y, a continuación, haga clic en **Finalizar**.
8. Seleccione **Back up Now**.
9. En la página Backup, realice los siguientes pasos:
   a. Si hay varias políticas asociadas con el recurso, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
   b. Haga clic en **copia de seguridad**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Realice un backup de los grupos de recursos de Oracle

Puede realizar el backup de los grupos de recursos que consten de varios recursos. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
   a. Si hay varias políticas asociadas con el grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
   b. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Restaurar y recuperar bases 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.

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.
4. En la vista Administrar copias, seleccione **Copias de seguridad** en el sistema de almacenamiento

primario.

5. Seleccione el backup en la tabla y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
   a. Seleccione RAC si seleccionó un backup de una base de datos en el entorno RAC.
   b. Realice las siguientes acciones:
      i. Seleccione **Todos los archivos de datos** si desea restaurar solo los archivos de la base de datos.
      ii. Seleccione **Tablespaces** si desea restaurar solo los tablespaces.
      iii. Seleccione **Redo log files** si desea restaurar los archivos redo log de las bases de datos en espera de Data Guard o Active Data Guard.
      iv. Seleccione **Pluggable databases** y especifique las PDB que desea restaurar.
      v. Seleccione * tablespaces de base de datos conectables (PDB)* y, a continuación, especifique la PDB y los tablespaces de esa PDB que desea restaurar.
      vi. Seleccione **Restaurar la base de datos en el mismo host donde se creó la copia de seguridad** si desea restaurar la base de datos en el mismo servidor SQL donde se realizan las copias de seguridad.
      vii. Seleccione **Restaurar la base de datos a un host alternativo** si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o en otro donde se realicen las copias de seguridad.
      viii. 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.
      ix. 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 Restore Scope, seleccione una de las siguientes opciones:
   a. Seleccione **All Logs** si desea recuperar la última transacción.
   b. Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico.
   c. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
   d. Seleccione **No recovery** si no desea recuperar.
   e. Seleccione **Especificar ubicaciones de archive log externas** si desea especificar la ubicación de los archivos archive log externos.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico

Puede restaurar un subconjunto de espacios de tablas que se hayan dañado o borrado sin que el resto de espacios de tablas de la base de datos se vea afectado. SnapCenter utiliza RMAN para realizar una recuperación puntual (PITR) de los tablespaces.

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 del tipo instancia única (multitenant).
4. En la vista Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento.

   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. Seleccione **RAC** si ha seleccionado una copia de seguridad de una base de datos en el entorno RAC.
   b. Seleccione **Tablespaces** si desea restaurar solo los tablespaces.
   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 Restore Scope, seleccione una de las siguientes opciones:
   a. Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico.
   b. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el proceso de restauración mediante la página **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.

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 del tipo instancia única (multitenant).
4. En la vista Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento.

   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. Seleccione **RAC** si ha seleccionado una copia de seguridad de una base de datos en el entorno RAC.
   b. Según si desea restaurar la PDB o los espacios de tablas en una PDB, realice una de las acciones:
      - Seleccione **Pluggable databases (PDBs)** si desea restaurar una PDB.
      - Seleccione **Pluggable database (PDB) tablespaces** si desea restaurar los espacios de tabla en una PDB.
7. En la página Restore Scope, seleccione una de las siguientes opciones:
   a. Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico.
   b. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el proceso de restauración mediante la página **Monitor** > **Jobs**.

Clone el backup de 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. Los clones creados son clones gruesos y se crean en el pool de capacidad primario.

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.
4. En la página Manage Copies view, seleccione el backup en el sistema de almacenamiento principal.
5. Seleccione la copia de seguridad de datos y, a continuación, haga clic en .
6. En la página Name, seleccione si desea clonar una base de datos (CDB o no CDB) o clonar una base de datos conectables (PDB).
7. En la página Locations, especifique los detalles necesarios.

   Si los volúmenes de ANF de la base de datos de Oracle están configurados en un pool de CAPACIDAD de CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

   Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

8. En la página Credentials, realice una de las siguientes acciones:
   a. Para el nombre de credencial para el usuario sys, seleccione la credencial que se utilizará para definir la contraseña de usuario sys de la base de datos clonada.
   b. Para el nombre de credencial de instancia de ASM, seleccione **Ninguno** si la autenticación del sistema operativo está activada para conectarse a la instancia de ASM en el host del clon.

De lo contrario, seleccione la credencial de Oracle ASM configurada con el usuario «sys» o un usuario con el privilegio «sysasm» aplicable al host de clonado.

9. En la página Pre-Ops, especifique la ruta y los argumentos de los scripts previos, y 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.
10. En la página Post-Ops, se seleccionan por defecto **Recover database** y **Until Cancel** para realizar la recuperación de la base de datos clonada.
    a. Si selecciona **Until Cancel**, SnapCenter realiza la recuperación mediante el montaje de la última copia de seguridad de registros que tiene la secuencia ininterrumpida de registros de archivos después de esa copia de seguridad de datos que se seleccionó para la clonación.
    b. Si selecciona **Fecha y hora**, SnapCenter recupera la base de datos hasta una fecha y hora especificadas.
    c. Si selecciona **Until SCN**, SnapCenter recupera la base de datos hasta un SCN especificado.
    d. Si selecciona **Especificar ubicaciones de archive log externas**, SnapCenter identifica y monta el número óptimo de copias de seguridad de log según el SCN especificado o la fecha y hora seleccionadas.
    e. Por defecto, la casilla de verificación **Crear nuevo DBID** está seleccionada para generar un número único (DBID) para la base de datos clonada diferenciándola de la base de datos de origen.

       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.

    f. Active la casilla de verificación **Create tempfile for temporary tablespace** si desea crear un archivo temporal para el tablespace temporal por defecto de la base de datos clonada.
    g. En **Introduzca las entradas sql que se aplicarán cuando se cree el clon**, agregue las entradas sql que desea aplicar cuando se cree el clon.
    h. En **Introduzca los scripts que se ejecutarán después de la operación de clonación**, especifique la ruta de acceso y los argumentos del postscript que desea ejecutar después de la operación de clonación.
11. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
12. Revisa el resumen y luego selecciona **Finalizar**.
13. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

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 Recursos, seleccione **Base de datos** o **Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos del tipo instancia única (multitenant).

4. En la página Manage Copies view, seleccione el backup en el sistema de almacenamiento principal.
5. Seleccione el backup y, a continuación, haga clic en .
6. En la página Nombre, seleccione **PDB Clone** y especifique los otros detalles.
7. En la página Locations, especifique los detalles necesarios.
8. En la página Pre-Ops, especifique la ruta y los argumentos de los scripts previos, y 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.
9. En la página Post-Ops, se selecciona **Until Cancel** de forma predeterminada para realizar la recuperación de la base de datos clonada.
    a. Si selecciona **Until Cancel**, SnapCenter realiza la recuperación mediante el montaje de la última copia de seguridad de registros que tiene la secuencia ininterrumpida de registros de archivos después de esa copia de seguridad de datos que se seleccionó para la clonación.
    b. Si selecciona **Fecha y hora**, SnapCenter recupera la base de datos hasta una fecha y hora especificadas.
    c. Si selecciona **Especificar ubicaciones de archive log externas**, SnapCenter identifica y monta el número óptimo de copias de seguridad de log según el SCN especificado o la fecha y hora seleccionadas.
    d. Por defecto, la casilla de verificación **Crear nuevo DBID** está seleccionada para generar un número único (DBID) para la base de datos clonada diferenciándola de la base de datos de origen.

       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.

    e. Active la casilla de verificación **Create tempfile for temporary tablespace** si desea crear un archivo temporal para el tablespace temporal por defecto de la base de datos clonada.
    f. En **Introduzca las entradas sql que se aplicarán cuando se cree el clon**, agregue las entradas sql que desea aplicar cuando se cree el clon.
    g. En **Introduzca los scripts que se ejecutarán después de la operación de clonación**, especifique la ruta de acceso y los argumentos del postscript que desea ejecutar después de la operación de clonación.
10. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revisa el resumen y luego selecciona **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

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 respaldados por un backup en almacenamiento primario como copias Snapshot, y en almacenamiento secundario mediante las tecnologías 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 ofrece información sobre el estado de protección para almacenamiento principal y secundario de Snapshots. 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 backup puede tener varias copias Snapshot asociadas y el número reflejará la misma. Esto se aplica tanto a las snapshots 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 de almacenamiento para el almacenamiento primario es la proporción de capacidad lógica (ahorro en clones y snapshots más almacenamiento consumido) con respecto a la capacidad física del almacenamiento principal. 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.

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**.

resultado

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.

Antes de empezar

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. 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. En la página Role Details, modifique los permisos o anule la asignación de los miembros según sea necesario.
2. Haga clic en **Enviar**.

Modificar usuarios y grupos

Es posible modificar usuarios o grupos de SnapCenter para modificar sus roles y activos.

Antes de empezar

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 compatibles con NetApp	Para DB2	Para PostgreSQL	Para MySQL
Añada los hosts e instale el paquete de plugins	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Actualizar la información de ESXi para un host	No	Sí	No	No	No	No	No	No	No
Suspenda las programaciones y coloque los hosts en modo de mantenimiento	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Añadir, actualizar o quitar plugins para modificar hosts	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Quite hosts de SnapCenter	Sí	Sí	Sí	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 compatibles con NetApp	Para DB2	Para PostgreSQL	Para MySQL
Iniciar servicios de plugins (solo aplicable a los plugins que se ejecutan en el host de Windows)	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Aprovisione los discos	No	No	Sí	No	No	No	No	No	No
Gestione los recursos compartidos de SMB	No	No	Sí	No	No	No	No	No	No
Gestionar los iGroups	No	No	Sí	No	No	No	No	No	No
Gestionar sesiones iSCSI	No	No	Sí	No	No	No	No	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**.

resultado

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 el icono 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 el icono 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.

resultado

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
Determine si hay recursos disponibles para backup	Sí	Sí	Sí	Sí	Sí
Llevar a cabo un backup bajo demanda de un recurso	Sí	Sí	Sí	Sí	Sí
Restaurar desde backups	Sí	Sí	Sí	Sí	Sí
Clonar backups	No	Sí	Sí	Sí	Sí
Gestionar backups	Sí	Sí	Sí	Sí	Sí
Gestionar clones	No	Sí	Sí	Sí	Sí
Gestionar políticas	Sí	Sí	Sí	Sí	Sí
Gestionar conexiones de almacenamiento	Sí	Sí	Sí	Sí	Sí
Montar backups	No	No	No	Sí	No
Desmontar backups	No	No	No	Sí	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
Ver detalles	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 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. 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.
Quite o cambie un tipo de programación	Realice lo siguiente: 1. Desvincule la política de cada recurso o grupo de recursos que use dicha política. 2. Modifique el tipo de programación. 3. Asocie la política otra vez a todos los recursos y grupos de recursos. 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.

Antes de empezar

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: Seleccione la casilla de verificación **Eliminar copias de seguridad y desvincular políticas asociadas con este grupo de recursos** para eliminar todas las copias de seguridad, metadatos, políticas e instantáneas asociadas 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.

Antes de empezar

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 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.

Quitar la protección

Eliminar protección elimina todos los backups y desvincula todas las políticas. Antes de quitar la protección, debe asegurarse de que los backups no estén montados y que no haya clones asociados con 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 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. Seleccione la copia de seguridad y haga clic en **Eliminar protección**.

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.

Gestionar tareas de backup programadas

A partir de la versión SnapCenter 6.0.1, se ha introducido un nuevo parámetro **JobConcurrencyThreshold** que establece un umbral para el número de trabajos programados que se pueden ejecutar en un momento dado. Esto le permite controlar el número de copias de seguridad que desea ejecutar en función de la configuración de hardware de su sistema.

El valor predeterminado asignado a **JobConcurrencyThreshold** es 0 y está desactivado. Se puede habilitar mediante la asignación de un valor, si se observa la degradación del rendimiento durante la ventana de backup programado.

Si habilita **JobConcurrencyThreshold** para administrar trabajos simultáneos, SnapCenter no le permitirá controlar el orden de las copias de seguridad y es posible que las copias de seguridad no se activen al mismo tiempo especificado en el programa.

Pasos

1. Configure el valor del parámetro *JobConcurrencyThreshold* ubicado en *C:\Archivos de programa\NetApp\SnapCenter WebApp\SnapManager.web.ui.dll.config*.
2. Recicle el pool de aplicaciones de SnapCenter haciendo clic en IIS > Pools de aplicaciones > SnapCenter > Reiniciar.
3. Reinicie el servicio web de SnapCenter haciendo clic en IIS > Sitios > SnapCenter > Reiniciar.

Gestionar trabajos obsoletos

Los trabajos obsoletos se crean a partir de interrupciones en SnapCenter o a partir de actualizaciones de trabajos incorrectas. A partir de la versión SnapCenter 6.0.1, se incorpora una programación predefinida para borrar estos trabajos obsoletos que se han atascado durante más de 72 horas. Puede cambiar la frecuencia de programación editando el parámetro configurable **CleanUpStaleJobsIntervalHours**.

Puede activar la limpieza a petición ejecutando el programa desde **Monitor** > **Horarios** > **SnapCenter_StaleJobCleanUp**.

Pasos

1. Configure el valor del parámetro *CleanUpStaleJobsIntervalHours* ubicado en *C:\Archivos de programa\NetApp\SnapCenter WebApp\SnapManager.web.ui.dll.config*.
2. Recicle el pool de aplicaciones de SnapCenter haciendo clic en IIS > Pools de aplicaciones > SnapCenter > Reiniciar.
3. Reinicie el servicio web de SnapCenter haciendo clic en IIS > Sitios > SnapCenter > Reiniciar.

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.

Información relacionada

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, 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.
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.

Tipo de informe	Descripción
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.
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. 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.

Antes de empezar

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 snapshots de ONTAP.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

> El backup que se utilizó para realizar la operación de restauración de repositorio no se mostrará cuando se recuperen los backups del repositorio después de realizar la operación de restauración.

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.

Antes de empezar

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.
```

Información relacionada

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, 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.

Antes de empezar

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, 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. a. En la página Storage Connections, haga clic en el nombre SVM adecuado. b. Ejecute una de las siguientes acciones: ◦ 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. ◦ 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. 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. 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. a. En la página Storage Connections, haga clic en el nombre del clúster. b. En la página Modify Storage System, haga clic en el icono para editar junto a Username y modifique el nombre de usuario y la contraseña. c. Seleccione o borre la configuración de EMS y AutoSupport. 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.

Soporte PARA API REST

Todas las conexiones de los sistemas ASA, AFF o FAS a ONTAP se realizarán a través de ZAPI de forma predeterminada. La API REST se puede habilitar para versiones específicas de ONTAP.

SnapCenter aprovecha las API REST para realizar todas las operaciones en sistemas ASA r2, que no admiten ZAPI.

Puede modificar las claves de configuración en los siguientes archivos de configuración:

- IsRestEnabledForStorageConnection

  El valor predeterminado es FALSE.

- MinOntapVersionToUseREST

  El valor predeterminado es 9.13.1.

Habilite la conexión mediante la API de REST

1. Establezca IsRestEnabledForStorageConnection en true.
2. Añada la clave en SMCoreServiceHost.dll.config y SnapDriveService.dll.config tanto en los hosts del servidor como de plugins de Windows.

   <add key="IsRestEnabledForStorageConnection" value="true" />

Limite la conexión a través de la API de REST a una versión específica de ONTAP

1. Establezca el parámetro config MinOntapVersionToUseREST en TRUE.
2. Añada la clave en SMCoreServiceHost.dll.config y SnapDriveService.dll.config tanto en los hosts del servidor como de plugins de Windows.

   <add key="MinOntapVersionToUseREST" value="9.13.1" />

3. Reinicie el servicio de SmCore en el servidor y el servicio del plugin y SnapDrive en la máquina del plugin.

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 NetApp 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*.

Información relacionada

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, 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**, haz clic en **Software**.

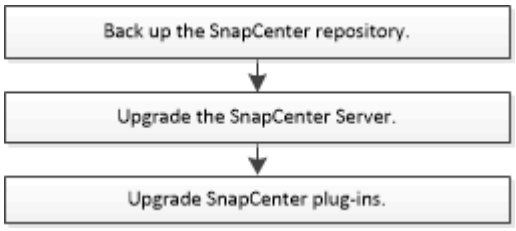
   La página Available Software muestra los paquetes de plugins y las versiones disponibles, así como su estado de instalación.

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 enumera las tareas que debe completar para actualizar los paquetes de complementos y servidores de SnapCenter .



Rutas de actualización admitidas

Esta sección muestra qué versiones de SnapCenter puede actualizar y qué versiones de complementos son compatibles.

Si actualiza SnapCenter Server a 6.2, actualice también los complementos a 6.2.

Si se encuentra en la versión de SnapCenter Server…	Puede actualizar directamente el servidor de SnapCenter a…	Versiones de plugins compatibles
6,0	6.0.1	• 6,0 • 6.0.1
	6,1	• 6,1
	6,2	• 6,2
6.0.1	6,1	• 6,1
	6,2	• 6,2
6,1	6,2	• 6,2

Para saber cómo actualizar el SnapCenter Plug-in for VMware vSphere, consulte "Actualice el plugin de SnapCenter para VMware vSphere" .

Actualice el servidor SnapCenter en el host de Windows

Debe actualizar el servidor SnapCenter para acceder a las últimas funciones y mejoras proporcionadas en la versión más reciente.

Antes de empezar

- Actualice el host del servidor SnapCenter con las últimas actualizaciones de Windows y asegúrese de que no haya reinicios del sistema pendientes.
- Asegúrese de que no haya otras operaciones en ejecución antes de iniciar la actualización.
- Instale el paquete de alojamiento ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) y PowerShell 7.4.2 o posterior.
- Realice una copia de seguridad de la base de datos del repositorio de SnapCenter (MySQL) después de asegurarse de que no haya ningún trabajo en ejecución. Se recomienda hacer esto antes de actualizar SnapCenter Server y el complemento de Exchange.

  Para obtener más información, consulte "Realice un backup del repositorio de SnapCenter".

- Realice una copia de seguridad de todos los archivos de configuración de SnapCenter modificados que haya modificado en el host del servidor SnapCenter o en el host del complemento.

  Ejemplos de archivos de configuración de SnapCenter: SnapDriveService.exe.config, SMCoreServiceHost.exe.config, etc.

- Si ha instalado varias versiones del complemento personalizado en SnapCenter 5.0, antes de actualizar a 6.0 o posterior, debe ejecutar los cmdlets de PowerShell para eliminar todas las versiones anteriores del complemento personalizado (excepto la última) del repositorio de SnapCenter (base de datos NSM).

- Correr `Open-SmConnection` e inicie sesión usando las credenciales del rol SnapCenterAdmin
- Correr `Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>`

  Para más información, consulte "La actualización a SnapCenter 6.0 o posterior falla" .

Acerca de esta tarea

- Durante la actualización, SnapCenter ejecuta un script SQL para actualizar los datos de Exchange en la base de datos NSM, convirtiendo el DAG y el nombre corto del host a FQDN. Esto solo se aplica si utiliza SnapCenter Server con el complemento Exchange.
- Si ha colocado manualmente el host del servidor en modo de mantenimiento, después de la actualización seleccione **Hosts** > **Activar programación** para sacar el host del servidor del modo de mantenimiento.
- Para las programaciones de backup y verificación existentes con scripts previos y posteriores habilitados en la política, las operaciones de backup seguirán funcionando después de la actualización.

  En la página **Detalles del trabajo**, un mensaje de advertencia recomienda que el cliente copie las secuencias de comandos en LA RUTA SCRIPTS y edite la directiva para proporcionar una ruta de acceso relativa a LA RUTA SCRIPTS_PATH. Para el trabajo de ciclo de vida de clon, aparece el mensaje de advertencia en el nivel de subtrabajo.

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 del host del complemento SnapCenter desde el Programador de tareas de Windows para restaurarlas si falla 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. Haga doble clic en el archivo .exe descargado para iniciar la actualización de SnapCenter Server.

   Después de iniciar la actualización, SnapCenter ejecuta comprobaciones previas. Si el sistema no cumple con los requisitos mínimos, SnapCenter muestra mensajes de error o advertencia. Puede ignorar las advertencias y continuar con la instalación, pero debe corregir cualquier error.

   SnapCenter continúa utilizando la contraseña de la base de datos del repositorio de MySQL Server existente proporcionada durante la instalación de la versión anterior de SnapCenter Server.

6. Seleccione **Actualizar**.

   Si selecciona **Cancelar** en cualquier etapa, SnapCenter detiene la actualización. No revertirá el servidor SnapCenter al estado anterior.

   Mejor práctica: Cierre sesión y vuelva a iniciarla, o abra un nuevo navegador para acceder a la interfaz de usuario de SnapCenter .

Después de terminar

- Si el plugin se instala con un usuario sudo, debe copiar las claves SHA224 disponibles en *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_PLUGINS_checksum.txt* para actualizar el archivo */etc/sudoers*.
- Debe ejecutar una detección nueva de los recursos que hay en el host del servidor.

  Si SnapCenter muestra el estado del host del servidor como detenido, espere un tiempo y realice una nueva detección. También puede cambiar el valor del parámetro **HostRefreshInterval** (el valor predeterminado es 3600 segundos) a cualquier valor superior a 10 minutos.

- Si la actualización falla, limpie la instalación fallida, reinstale la versión anterior de SnapCenter y restaure la base de datos NSM al estado en que se encontraba antes.
- Después de actualizar el host del servidor, también debe actualizar los plugins antes de añadir cualquier sistema de almacenamiento.

Actualice el servidor SnapCenter en el host Linux

Puede utilizar el archivo de instalación del servidor de SnapCenter para actualizar el servidor de SnapCenter.

- Pasos*
  1. Realice una de las acciones para actualizar el servidor SnapCenter.

Si desea ejecutar…	Realice lo siguiente…
Actualización no interactiva	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename>` Ejemplo: Sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log Los registros se almacenarán en */var/opt/snapcenter/logs*. Parámetros que se transferirán para la actualización: • DINSTALL_LOG_NAME: Nombre del archivo de registro donde se almacenarán los registros de instalación. • DUPGRADE: El valor predeterminado es 0. Especifique este parámetro y su valor como cualquier entero que no sea 0 para actualizar el servidor SnapCenter.
Instalación interactiva	`./snapcenter-linux-server-(el8/el9/sles15).bin` Se le pedirá que confirme la actualización. Introduzca un valor distinto de 0 para confirmar la actualización del servidor SnapCenter.

Debe cerrar sesión y, a continuación, iniciar sesión en SnapCenter, o bien cerrar y abrir un nuevo explorador para acceder a la interfaz gráfica de usuario de SnapCenter.

Actualizar los paquetes de complementos de SnapCenter

Los paquetes de complementos se distribuyen como parte de la actualización de SnapCenter . El procedimiento de actualización pone automáticamente sus hosts con complementos Windows, Linux o AIX en modo de mantenimiento. El modo de mantenimiento impide que el host del complemento ejecute cualquier tarea programada durante la actualización.

El sistema selecciona todos los complementos del paquete, pero actualiza solo los complementos que instalaste con la versión anterior de SnapCenter. El sistema no instala los complementos restantes. Utilice la opción **Añadir complementos** para instalar cualquier complemento nuevo.

Antes de empezar

- 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.

- Asegúrese de que PowerShell Core 7.4.2 esté instalado en el host del complemento de Windows.
- Asegúrese de que Java 11, Oracle Java y OpenJDK estén instalados en los hosts de complementos de Windows y Linux.
- 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.

- Realice una copia de seguridad de todos los archivos de configuración de SnapCenter modificados (como SnapDriveService.exe.config, SMCoreServiceHost.exe.config, etc.) en el host del servidor SnapCenter o en el host del complemento.

Acerca de esta tarea

Para el plugin de SnapCenter para Microsoft SQL Server, el plugin de SnapCenter para Microsoft Exchange Server y el plugin de SnapCenter para Microsoft Windows, es recomendable actualizar el servidor y los hosts del plugin a la versión más reciente para ejecutar LA RUTA_DE_SCRIPTS.

Para las programaciones de backup y verificación existentes con scripts previos y posteriores habilitados en la política, las operaciones de backup seguirán funcionando después de la actualización.

En la página **Detalles del trabajo**, un mensaje de advertencia recomienda que el cliente copie las secuencias de comandos en LA RUTA SCRIPTS y edite la directiva para proporcionar una ruta de acceso relativa a LA RUTA SCRIPTS_PATH. Para el trabajo de ciclo de vida de clon, aparece el mensaje de advertencia en el nivel de subtrabajo.

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 de complementos, haga clic en el nombre del host del complemento y realice lo siguiente:
     i. Haga clic en **más opciones**.
     ii. Seleccione **Omitir comprobaciones previas** si no desea validar si el host del plugin cumple con los requisitos para actualizar el plugin.

Si no selecciona **Omitir comprobaciones previas**, SnapCenter comprueba si el host del complemento cumple los requisitos. Si no se cumplen los requisitos, aparecerán mensajes de error o advertencia. 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* o los archivos de configuración de PowerShell ubicados en *C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ SnapCenter* para modificar los valores predeterminados. Si el error está relacionado con los parámetros restantes, deberá solucionar el problema y luego validar los requisitos nuevamente.

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 servicios relacionados se reinician durante la actualización del plugin.

Actualización tecnológica

Actualización tecnológica del host de servidor de SnapCenter

Cuando sea necesario actualizar el host de SnapCenter Server, puede instalar la misma versión de SnapCenter Server en el nuevo host y, a continuación, ejecutar las API para realizar backups del SnapCenter desde el servidor antiguo y restaurarlo en el nuevo servidor.

Pasos

1. Implemente el nuevo host y realice las siguientes tareas:
   a. Instale la misma versión del servidor de SnapCenter.
   b. (Opcional) Configurar certificados de CA y habilitar SSL bidireccional. Para obtener más información, consulte "Configurar certificado de CA" y.. "Configure y habilite SSL bidireccional".
   c. (Opcional) Configurar la autenticación multifactor. Para obtener más información, consulte "Habilite la autenticación multifactor".
2. Inicie sesión como usuario administrador de SnapCenter.
3. Cree un backup del servidor SnapCenter en el host anterior mediante la API: `/<snapcenter_version>/server/backup` O el cmdlet: *New-SmServerBackup*.

   Antes de realizar el backup, suspenda todos los trabajos programados y asegúrese de que no existan trabajos en ejecución.

   Si desea restaurar el backup en el servidor de SnapCenter que se está ejecutando en un nuevo dominio, antes de realizar un backup, debe añadir el usuario de dominio nuevo en el host anterior de SnapCenter y asignar el rol de administrador de SnapCenter.

4. Copie el backup del host anterior en el nuevo.
5. Restaure el backup del servidor SnapCenter en el nuevo host mediante la API: `/<snapcenter_version>/server/restore` O el cmdlet: *Restore-SmServerBackup*.

   Restore actualizará la nueva URL del servidor SnapCenter en todos los hosts de forma predeterminada. Si desea omitir la actualización, use el atributo *-SkipSMSURLInHosts* y actualice por separado la URL del servidor ejecutando mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.

   Si el host del plugin no puede resolver el nombre de host del servidor, inicie sesión en cada host del plugin y añada la entrada *etc/host* para la nueva IP en el formato <New IP> SC_Server_Name.

   Las entradas *etc/host* del servidor no se restaurarán. Puede restaurarlo manualmente desde el servidor antiguo.

   Si la copia de seguridad se restaura en el servidor SnpCenter que se ejecuta en un nuevo dominio y si desea seguir utilizando los usuarios de dominio antiguos, debe registrar el dominio antiguo en el nuevo

servidor SnapCenter.

> Si actualizó manualmente el archivo web.config en el antiguo host de SnapCenter, las actualizaciones no se copiarán en el nuevo host. Debe realizar los mismos cambios manualmente en el archivo web.config del nuevo host.

6. Si omitió la actualización de la URL del servidor de SnapCenter o alguno del host se encontraba inactivo durante el proceso de restauración, actualice el nuevo nombre de servidor en todos los hosts o los hosts especificados que gestiona SnapCenter mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.
7. Active los trabajos programados en todos los hosts desde el nuevo servidor de SnapCenter.

Actualización tecnológica de un nodo en un clúster F5

Puede realizar una actualización tecnológica de cualquier nodo del clúster F5 quitando el nodo y añadiendo el nodo nuevo. Si el nodo que necesita actualizarse está activo, convierta otro nodo del clúster como activo y a continuación quite el nodo.

Para obtener información sobre cómo añadir un nodo a un clúster F5, consulte "Configurar servidores SnapCenter para alta disponibilidad mediante F5".

> Si cambia la url del clúster F5, la url se puede actualizar en todos los hosts mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.

Desmantelamiento del antiguo host del servidor de SnapCenter

Es posible quitar el antiguo host de servidor de SnapCenter después de verificar que el nuevo servidor SnapCenter esté activo y en ejecución, y todos los hosts de plugins pueden comunicarse con el nuevo host de servidor de SnapCenter.

Realice una reversión al antiguo host del servidor de SnapCenter

En caso de cualquier problema, puede recuperar el antiguo host del servidor SnapCenter actualizando la URL del servidor SnapCenter en todos los hosts a través de la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.

Recuperación tras siniestros

Recuperación ante desastres en un host SnapCenter independiente

Puede realizar la recuperación ante desastres restaurando el backup del servidor en el nuevo host.

Antes de empezar

Asegúrese de tener una copia de seguridad del antiguo servidor SnapCenter.

Pasos

1. Implemente el nuevo host y realice las siguientes tareas:
   a. Instale la misma versión del servidor de SnapCenter.
   b. Configurar certificados de CA y activar SSL bidireccional. Para obtener más información, consulte "Configurar certificado de CA" y.. "Configure y habilite SSL bidireccional".

2. Copie el antiguo backup del servidor de SnapCenter en el nuevo host.
3. Inicie sesión como usuario administrador de SnapCenter.
4. Restaure el backup del servidor SnapCenter en el nuevo host mediante la API: `/<snapcenter_version>/server/restore` O el cmdlet: *Restore-SmServerBackup*.

   Restore actualizará la nueva URL del servidor SnapCenter en todos los hosts de forma predeterminada. Si desea omitir la actualización, use el atributo *-SkipSMSURLInHosts* y actualice por separado la URL del servidor mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.

   Si el host del plugin no puede resolver el nombre de host del servidor, inicie sesión en cada host del plugin y añada la entrada *etc/host* para la nueva IP en el formato <New IP> SC_Server_Name.

   Las entradas *etc/host* del servidor no se restaurarán. Puede restaurarlo manualmente desde el servidor antiguo.

5. Si omitió la actualización de la URL o alguno del host estaba inactivo durante el proceso de restauración, actualice el nuevo nombre del servidor en todos los hosts o los hosts especificados que SnapCenter gestiona mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.

Recuperación ante desastres del clúster SnapCenter F5

Puede realizar la recuperación ante desastres mediante la restauración del backup del servidor en el nuevo host y, a continuación, convirtiendo el host independiente en un clúster.

Antes de empezar

Asegúrese de tener una copia de seguridad del antiguo servidor SnapCenter.

Pasos

1. Implemente el nuevo host y realice las siguientes tareas:
   a. Instale la misma versión del servidor de SnapCenter.
   b. Configurar certificados de CA y activar SSL bidireccional. Para obtener más información, consulte "Configurar certificado de CA" y.. "Configure y habilite SSL bidireccional".
2. Copie el antiguo backup del servidor de SnapCenter en el nuevo host.
3. Inicie sesión como usuario administrador de SnapCenter.
4. Restaure el backup del servidor SnapCenter en el nuevo host mediante la API: `/<snapcenter_version>/server/restore` O el cmdlet: *Restore-SmServerBackup*.

   Restore actualizará la nueva URL del servidor SnapCenter en todos los hosts de forma predeterminada. Si desea omitir la actualización, use el atributo *-SkipSMSURLInHosts* y actualice por separado la URL del servidor mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.

   Si el host del plugin no puede resolver el nombre de host del servidor, inicie sesión en cada host del plugin y añada la entrada *etc/host* para la nueva IP en el formato <New IP> SC_Server_Name.

Las entradas *etc/host* del servidor no se restaurarán. Puede restaurarlo manualmente desde el servidor antiguo.

5. Si omitió la actualización de la URL o alguno del host estaba inactivo durante el proceso de restauración, actualice el nuevo nombre del servidor en todos los hosts o los hosts especificados que SnapCenter gestiona mediante la API: `/<snapcenter_version>/server/configureurl` O el cmdlet: *Set-SmServerConfig*.
6. Convierta el host independiente en clúster de F5.

   Para obtener información sobre cómo configurar F5, consulte "Configurar servidores SnapCenter para alta disponibilidad mediante F5".

Información relacionada

Para obtener información sobre las API, tiene que acceder a la página de Swagger. consulte "Cómo acceder a las API de REST con la página web de la API swagger".

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

Actualización tecnológica de los hosts de complementos de SnapCenter

Cuando los hosts del plugin de SnapCenter requieren una actualización, es necesario mover los recursos del host antiguo al nuevo. Cuando se agrega el nuevo host a SnapCenter, detectará todos los recursos, pero se tratará como recursos nuevos.

Acerca de esta tarea

Debe ejecutar la API o el cmdlet que tomará el nombre de host antiguo y el nuevo nombre de host como entrada, comparar los recursos por nombre y volver a vincular los objetos de recursos coincidentes del host antiguo al nuevo host. Los recursos coincidentes se marcarán como protegidos.

- El parámetro *IsDryRun* se define en True de forma predeterminada e identifica los recursos coincidentes del host antiguo y nuevo.

  Después de verificar los recursos coincidentes, debe establecer el parámetro *IsDryRun* en False para volver a vincular los objetos de los recursos coincidentes del host anterior al nuevo host.

- El parámetro *AutoMigrateManuallyAddedResources* se establece en True de forma predeterminada, y esto copia automáticamente los recursos que se agregaron manualmente del host antiguo al nuevo host.

  El parámetro *AutoMigrateManuallyAddedResources* sólo se aplica a recursos de Oracle y SAP HANA.

- Se debe utilizar el parámetro *SQLInstanceMapping* si el nombre de la instancia es diferente entre el host antiguo y el nuevo. Si es una instancia por defecto, utilice *DEFAULT_INSTANCE* como nombre de instancia.

La actualización tecnológica es compatible con los siguientes complementos de SnapCenter:

- Plugin de SnapCenter para Microsoft SQL Server

- Si las bases de datos de SQL se protegen en el nivel de la instancia y, como parte de la actualización tecnológica del host, solo se mueven los recursos parciales a un nuevo host, la protección de nivel de instancia existente se convierte en protección de grupos de recursos, y las instancias de ambos hosts se añaden al grupo de recursos.
- Si se usa un host SQL (por ejemplo, host1) como programador o servidor de verificación para recursos de otro host (por ejemplo, host2), al realizar la actualización tecnológica en host1, la programación o los detalles de verificación no se migrarán y se seguirán ejecutando en host1. Si tiene que modificar, debe cambiarlo manualmente en los respectivos hosts.
- Si utiliza la configuración de instancias de clústeres de conmutación por error de SQL (FCI), puede realizar la actualización técnica añadiendo el nuevo nodo al clúster de FCI y actualizando el host del plugin en SnapCenter.
- Si utiliza una configuración de SQL Availability Group (AG), no es necesaria una actualización técnica. Puede añadir el nuevo nodo a AG y actualizar el host en SnapCenter.

- Plugin de SnapCenter para Windows
- Plugin de SnapCenter para base de datos de Oracle

  Si utiliza la configuración de Real Application Cluster (RAC) de Oracle, puede realizar la actualización técnica añadiendo el nuevo nodo al clúster de RAC y actualizando el host del plugin en SnapCenter.

- Plugin de SnapCenter para base de datos SAP HANA

Los casos de uso admitidos son:

- Migración de recursos de un host a otro.
- Migrar recursos desde varios hosts a uno o menos hosts.
- Migración de recursos de un host a varios hosts.

Los escenarios admitidos son:

- El nuevo host tiene un nombre diferente al anterior
- Se cambió el nombre del host existente

Antes de empezar

Como este flujo de trabajo modifica los datos del repositorio de SnapCenter, se recomienda realizar una copia de seguridad del repositorio de SnapCenter. En caso de cualquier problema con los datos, el repositorio de SnapCenter puede revertirse a estado antiguo mediante el backup.

Para obtener más información, consulte "Realice un backup del repositorio de SnapCenter".

Pasos

1. Despliegue el nuevo host e instale la aplicación.
2. Suspenda las programaciones del host antiguo.
3. Mueva los recursos necesarios del host antiguo al nuevo.
   a. Obtenga las bases de datos necesarias en el nuevo host desde el mismo almacenamiento.
      - Asegúrese de que el almacenamiento esté asignado a la misma unidad o a la misma ruta de montaje que el host anterior. Si el almacenamiento no se asigna correctamente, los backups creados en el host antiguo no se pueden usar para la restauración.

De forma predeterminada, Windows asigna automáticamente la siguiente unidad disponible.

- Si el almacenamiento de recuperación de desastres está habilitado, el almacenamiento correspondiente debe montarse en el nuevo host.

b. Compruebe la compatibilidad si hay un cambio en la versión de la aplicación.

c. Sólo para el host del plugin de Oracle, asegúrese de que los UID y GID de Oracle y de los usuarios de grupo sean los mismos que los del host antiguo.

Para obtener más información, consulte:

- "Cómo migrar la base de datos de SQL del host antiguo al nuevo host"
- "Cómo migrar la base de datos de Oracle del host antiguo al nuevo host"
- "Cómo convertir la base de datos SAP HANA en un nuevo host"

4. Añada el nuevo host a SnapCenter.
5. Verifique si se han detectado todos los recursos.
6. Ejecute la API de actualización del host: `/<snapcenter_version>/techrefresh/host` O el cmdlet: *Invoke-SmTechRefreshHost*.

La ejecución en seco está activada de forma predeterminada y se identifican los recursos coincidentes que se van a volver a enlazar. Para verificar los recursos, puede ejecutar la API: '/jobs/{jobid}' o el cmdlet *Get-SmJobSummaryReport*.

Si ha migrado los recursos desde varios hosts, debe ejecutar la API o el cmdlet para todos los hosts. Si la unidad o la ruta de montaje del nuevo host no es la misma que el host anterior, las siguientes operaciones de restauración fallarán:

- Se produce un error en la restauración sin movimiento de SQL. Sin embargo, la función RTAL se puede aprovechar.
- Se producirá un error en la restauración de las bases de datos de Oracle y SAP HANA.

Si desea migrar a varios hosts, debe realizar todos los pasos del paso 1 para todos los hosts.

Puede ejecutar la API o el cmdlet en el mismo host varias veces, solo se volverá a enlazar si hay un nuevo recurso identificado.

7. (Opcional) Quita el host o los hosts anteriores de SnapCenter.

Información relacionada

Para obtener información acerca de las API , tendrá que acceder a la página de Swagger. consulte "Cómo acceder a las API de REST con la página web de la API swagger".

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

Actualización tecnológica del sistema de almacenamiento

Cuando se actualiza el almacenamiento tecnológico, los datos se migran al nuevo almacenamiento y los hosts de aplicaciones se montan con nuevo almacenamiento. El flujo de trabajo de backup de SnapCenter identifica el nuevo almacenamiento y crea la instantánea si el nuevo almacenamiento se registra en SnapCenter.

Es posible realizar la restauración, el montaje y la clonación en los nuevos backups creados después de la actualización del almacenamiento. Sin embargo, estas operaciones fallarán cuando se realicen en los backups que se crearon antes de la actualización del almacenamiento, ya que los backups tienen los detalles del almacenamiento antiguo. Debe ejecutar la API o el cmdlet de actualización tecnológica del almacenamiento para actualizar los backups antiguos en SnapCenter con los nuevos detalles del almacenamiento.

La actualización tecnológica es compatible con los siguientes complementos de SnapCenter:

- Plugin de SnapCenter para Microsoft SQL Server
- Plugin de SnapCenter para Windows
- Plugin de SnapCenter para base de datos de Oracle
- Plugin de SnapCenter para base de datos SAP HANA
- Plugin de SnapCenter para Microsoft Exchange Server

Los casos de uso admitidos son:

- Actualización del almacenamiento principal

  La actualización tecnológica de almacenamiento es compatible para sustituir el almacenamiento principal por nuevo almacenamiento. No puede convertir el almacenamiento secundario existente en un almacenamiento primario.

- Actualización del almacenamiento secundario

Actualice las copias de seguridad del almacenamiento primario

Cuando se actualiza la tecnología del almacenamiento, es conveniente ejecutar la API o el cmdlet de actualización técnica del almacenamiento para actualizar los backups antiguos en SnapCenter con los nuevos detalles del almacenamiento.

Antes de empezar

Como este flujo de trabajo modifica los datos del repositorio de SnapCenter, se recomienda realizar una copia de seguridad del repositorio de SnapCenter. En caso de cualquier problema con los datos, el repositorio de SnapCenter puede revertirse a estado antiguo mediante el backup.

Para obtener más información, consulte "Realice un backup del repositorio de SnapCenter".

Pasos

1. Migrar los datos de un almacenamiento antiguo al nuevo.

   Para obtener más información sobre cómo migrar, consulte:

   - "Cómo migrar los datos a un nuevo almacenamiento"
   - "¿Cómo puedo copiar un volumen y conservar todas las copias Snapshot?"

2. Ponga el host en modo de mantenimiento.
3. Montar el nuevo almacenamiento en los respectivos hosts y resaltar las bases de datos.

   El nuevo almacenamiento debe conectarse al host de la misma manera que antes. Por ejemplo, si estaba conectado como SAN, necesita conectarse como SAN.

   El nuevo almacenamiento debe montarse en la misma unidad o ruta que el almacenamiento anterior.

4. Verifique que todos los recursos estén activos y en ejecución.
5. Añada el nuevo almacenamiento en SnapCenter.

   Compruebe que tiene un nombre de SVM único en los clústeres de SnapCenter. Si utiliza el mismo nombre de SVM en el nuevo almacenamiento y si todos los volúmenes de la SVM pueden migrarse antes de ejecutar la actualización de almacenamiento, después, se recomienda eliminar la SVM en el clúster antiguo y volver a detectar el clúster antiguo en SnapCenter que eliminará la SVM de la caché.

6. Ponga el host en modo de producción.
7. En SnapCenter, cree un backup de los recursos cuyo almacenamiento se migra. Es necesario un nuevo backup para que SnapCenter identifique el último espacio de almacenamiento necesario para actualizar los metadatos de los backups antiguos existentes.

   Siempre que se conecte un nuevo LUN al host, tendrá un nuevo número de serie. Durante el descubrimiento del sistema de archivos de Windows, SnapCenter tratará cada número de serie único como nuevo recurso. Durante la actualización de la tecnología de almacenamiento cuando el LUN de un nuevo almacenamiento se conecta al host con la misma letra o ruta de unidad, la detección del sistema de archivos de Windows en SnapCenter marcará el recurso existente como eliminado, incluso si se monta con la misma letra o ruta de la unidad y mostrará el nuevo LUN como nuevo recurso. Cuando el recurso se marca como eliminado, no se considerará para la actualización de la tecnología de almacenamiento en SnapCenter, y se perderán todos los backups del recurso anterior. Cuando se produce una actualización del almacenamiento, en el caso de recursos del sistema de archivos Windows, no se debe realizar la detección de recursos antes de ejecutar la API o el cmdlet de actualización de almacenamiento.

8. Ejecute la API de actualización del almacenamiento: `/<snapcenter_version>/techrefresh/primarystorage` O el cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   Si el recurso se configura con una política de replicación habilitada, el backup más reciente después de la actualización de almacenamiento debe tener detalles del almacenamiento secundario.

   a. Si utiliza la configuración de instancias de clúster de conmutación por error (FCI) de SQL, las copias de seguridad se mantienen en el nivel del clúster. Debe proporcionar el nombre del clúster como entrada para la actualización de la tecnología de almacenamiento.
   b. Si utiliza una configuración de SQL Availability Group (AG), los backups se mantienen en el nivel de nodo. Debe proporcionar el nombre de nodo como entrada para la actualización de la tecnología de almacenamiento.
   c. Si utiliza la configuración de Oracle Real Application Clusters (RAC), puede realizar la actualización de la tecnología de almacenamiento en cualquier nodo.

El atributo *IsDryRun* se establece en True de forma predeterminada. Así, se identificarán los recursos para los que se actualiza el almacenamiento. Para ver el recurso y los detalles del almacenamiento modificados, debe ejecutar la API: '<SnapCenter_version>/jobs/{jobid}' o el cmdlet *Get-SmJobSummaryReport*.

9. Después de verificar los detalles del almacenamiento, establezca el atributo *IsDryRun* en False y ejecute la API de actualización del almacenamiento `/<snapcenter_version>/techrefresh/primarystorage` : O el cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   Esto actualizará los detalles de almacenamiento en las copias de seguridad antiguas.

   Puede ejecutar la API o el cmdlet en el mismo host varias veces y actualizará los detalles del almacenamiento de los backups anteriores solamente si se actualiza el almacenamiento.

   > La jerarquía de clones no se puede migrar en ONTAP. Si el almacenamiento que se migra tiene metadatos de clonado en SnapCenter, el recurso clonado se marcará como recurso independiente. Los clones de los metadatos del clon se eliminarán de forma recursiva.

10. (Opcional) Si todas las snapshots no se mueven del almacenamiento primario antiguo a un nuevo almacenamiento primario, ejecute la siguiente API: `/<snapcenter_version>/hosts/primarybackupsexistencecheck` O el cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    Esto realizará la comprobación de existencia de instantáneas en el nuevo almacenamiento primario y marcará los respectivos backups que no están disponibles para ninguna operación en SnapCenter.

Actualice los backups del almacenamiento secundario

Cuando se actualiza la tecnología del almacenamiento, es conveniente ejecutar la API o el cmdlet de actualización técnica del almacenamiento para actualizar los backups antiguos en SnapCenter con los nuevos detalles del almacenamiento.

Antes de empezar

Como este flujo de trabajo modifica los datos del repositorio de SnapCenter, se recomienda realizar una copia de seguridad del repositorio de SnapCenter. En caso de cualquier problema con los datos, el repositorio de SnapCenter puede revertirse a estado antiguo mediante el backup.

Para obtener más información, consulte "Realice un backup del repositorio de SnapCenter".

Pasos

1. Migrar los datos de un almacenamiento antiguo al nuevo.

   Para obtener más información sobre cómo migrar, consulte:

   - "Cómo migrar los datos a un nuevo almacenamiento"
   - "¿Cómo puedo copiar un volumen y conservar todas las copias Snapshot?"

2. Establezca la relación de SnapMirror entre el almacenamiento principal y el nuevo almacenamiento secundario, y asegúrese de que el estado de la relación sea correcto.
3. En SnapCenter, cree un backup de los recursos cuyo almacenamiento se migra.

   Es necesario un nuevo backup para que SnapCenter identifique el último espacio de almacenamiento y se

utilizará para actualizar los metadatos de los backups anteriores existentes.

> Debe esperar hasta que se complete esta operación. Si continúa con el siguiente paso antes de que finalice, SnapCenter perderá por completo metadatos de Snapshot secundarias antiguas.

4. Después de crear correctamente el backup de todos los recursos en un host, ejecute la API de actualización del almacenamiento secundario `/<snapcenter_version>/techrefresh/secondarystorage` o el cmdlet: *Invoke-SmTechRefreshSecondaryStorage*.

   Esto actualizará los detalles del almacenamiento secundario de los backups anteriores en el host dado.

   Si desea ejecutar esto a nivel de recurso, haga clic en **Actualizar** para cada recurso para actualizar los metadatos de almacenamiento secundario.

5. Después de actualizar correctamente los backups antiguos, puede romper la relación de almacenamiento secundario anterior con el primario.

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.
- 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 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*. 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 se debe a que las copias Snapshot se eliminan de cada controladora y se limpian los metadatos.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. En la página **Hosts**, haz clic en **Hosts administrados**.
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.

Antes de empezar

- 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*. Alternativamente, 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*. Alternativamente, también puede consultar el "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.

Antes de empezar

- 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 en el host de Windows

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.

Antes de empezar

- 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.

Desinstale el servidor SnapCenter en el host Linux

Si no desea utilizar más el servidor de SnapCenter para gestionar trabajos de protección de datos, puede desinstalar SnapCenter Server. Al desinstalar el servidor SnapCenter se quitan todos sus componentes.

Pasos

1. Realice una de las acciones para desinstalar el servidor SnapCenter.

Si desea ejecutar…	Realice lo siguiente…
Desinstalación no interactiva	`$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1` Ejemplo: Sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall
Desinstalación interactiva	`$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall` Introduzca cualquier valor distinto de 0 en la entrada de confirmación para confirmar la desinstalación.

Automatización mediante API de REST

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 disponible en *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* para ver la documentación de la 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
- Plugin para base de datos de Oracle

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"

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.

Características operativas básicas

Mientras QUE REST establece un conjunto común de tecnologías y prácticas recomendadas, los detalles de cada API pueden variar en función de las opciones de diseño.

Transacción de API de solicitud y respuesta

Cada llamada de API REST se realiza como una solicitud HTTP al sistema de SnapCenter Server, lo que genera una respuesta asociada al cliente. Este par de solicitudes y respuestas se considera una transacción de API.

Antes de utilizar la API, debería estar familiarizado con las variables de entrada disponibles para controlar una solicitud y el contenido de la salida de la respuesta.

Compatibilidad con operaciones CRUD

Se accede a cada uno de los recursos disponibles a través de la API REST de SnapCenter en función del modelo CRUD:

- Cree
- Lea
- Actualizar
- Eliminar

Para algunos de los recursos, solo se admite un subconjunto de las operaciones.

Identificadores de objeto

A cada instancia u objeto de recurso se le asigna un identificador único cuando se crea. En la mayoría de los casos, el identificador es un UUID de 128 bits. Estos identificadores son globalmente únicos dentro de un servidor SnapCenter específico.

Después de emitir una llamada API que crea una nueva instancia de objeto, se devuelve una dirección URL con el identificador asociado al llamante en la cabecera de ubicación de la respuesta HTTP. Puede extraer el identificador y utilizarlo en llamadas posteriores cuando haga referencia a la instancia del recurso.

El contenido y la estructura interna de los identificadores de objeto pueden cambiar en cualquier momento. Solo se deben usar los identificadores en las llamadas API aplicables según sea necesario cuando se hacen referencia a los objetos asociados.

Instancias y colecciones de objetos

Dependiendo de la ruta de recursos y del método HTTP, una llamada API puede aplicarse a una instancia de objeto específica o a una colección de objetos.

Operaciones síncronas y asíncronas

SnapCenter realiza una solicitud HTTP recibida de un cliente de forma síncrona o asíncrona.

Procesamiento sincrónico

SnapCenter realiza la solicitud inmediatamente y responde con un código de estado HTTP de 200 o 201 si se realiza correctamente.

Cada solicitud que utilice EL método GET se realiza siempre de forma síncrona. Además, las solicitudes que utilizan POST están diseñadas para ejecutarse de forma síncrona si se espera que se completen en menos de dos segundos.

Procesamiento asíncrono

Si una solicitud asíncrona es válida, SnapCenter crea una tarea en segundo plano para procesar la solicitud y un objeto de trabajo para anclar la tarea. El código de estado HTTP 202 se devuelve al autor de la llamada junto con el objeto de trabajo. Debe recuperar el estado del trabajo para determinar si el trabajo es correcto o fallido.

Las solicitudes que utilizan los métodos POST y DELETE están diseñadas para ejecutarse asincrónicamente

si se espera que tarden más de dos segundos en completarse.

Seguridad

La seguridad proporcionada con la API DE REST se basa principalmente en las funciones de seguridad existentes disponibles con SnapCenter. La API utiliza la siguiente seguridad:

Seguridad de la capa de transporte

Todo el tráfico enviado por la red entre el servidor SnapCenter y el cliente suele cifrarse con TLS, según las opciones de configuración de SnapCenter.

Autenticación HTTP

En un nivel HTTP, se utiliza la autenticación básica para las transacciones de API. A cada solicitud se agrega un encabezado HTTP con el nombre de usuario y la contraseña en una cadena base64.

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
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.

Codificación	Descripción
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 con SnapCenter Server y los plugins

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 usar esta 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 las API para realizar diferentes operaciones.

- Recupere todos los dominios en SnapCenter
- recuperar detalles de un dominio específico
- registre o cancele el registro de un dominio
- modificar un dominio

Trabajos

Puede usar las API para realizar diferentes operaciones.

- Recupere todos los trabajos en SnapCenter
- recuperar el estado de un trabajo
- cancelar o detener un trabajo

Configuración

Puede usar las API para realizar diferentes operaciones.

- registre, modifique o quite una credencial
- Muestra la información de credenciales registrada en el servidor SnapCenter

- configurar los ajustes de notificación
- Recupera información sobre el servidor SMTP actualmente configurado para enviar notificaciones por correo electrónico y muestra el nombre del servidor SMTP, el nombre de los destinatarios y el nombre del remitente
- Muestra la configuración de la autenticación multifactor (MFA) del inicio de sesión en SnapCenter Server
- Habilite o deshabilite y configure la MFA para el inicio de sesión de SnapCenter Server
- Cree el archivo de configuración necesario para configurar la MFA

Hosts

Puede usar las API para realizar diferentes operaciones.

- Consulte todos los hosts SnapCenter
- Quite uno o varios hosts de SnapCenter
- recuperar un host por nombre
- recuperar todos los recursos de un host
- Recupere un recurso mediante el ID de recurso
- recupere los detalles de configuración del plugin
- configure el host del plugin
- Recupere todos los recursos del host del plugin para Microsoft SQL Server
- Recuperar todos los recursos del plugin para el host de la base de datos de Oracle
- recupere todos los recursos del plugin para el host de aplicaciones personalizadas
- Recupere todos los recursos del plugin para el host SAP HANA
- recupere los plugins instalados
- instale plugins en un host existente
- actualice el paquete del host
- quite los plugins de un host existente
- añadir el plugin en un host
- añadir o modificar el host
- Obtenga la firma del host Linux
- Registre la firma del host Linux
- ponga el host en modo de mantenimiento o producción
- inicie o reinicie los servicios de plugin en el host
- cambiar el nombre de un host

Recursos

Puede usar las API para realizar diferentes operaciones.

- recupere todos los recursos
- Recupere un recurso mediante el ID de recurso

- Recupere todos los recursos del host del plugin para Microsoft SQL Server
- Recuperar todos los recursos del plugin para el host de la base de datos de Oracle
- recupere todos los recursos del plugin para el host de aplicaciones personalizadas
- Recupere todos los recursos del plugin para el host SAP HANA
- Recupere un recurso de Microsoft SQL Server mediante una clave
- recupere un recurso personalizado mediante una clave
- modificar un recurso del plugin para un host de aplicación personalizada
- quite un recurso del plugin para el host de aplicación personalizada mediante una clave
- Recupere un recurso de SAP HANA mediante una clave
- Modificar un recurso del plugin para el host de SAP HANA
- Quite un recurso del plugin para el host SAP HANA mediante una clave
- Recupere un recurso de Oracle con una clave
- Cree un recurso de volumen de aplicaciones de Oracle
- Modificar un recurso de volumen de aplicaciones de Oracle
- Quite un recurso de volumen de aplicaciones de Oracle mediante una clave
- Recupere los detalles secundarios del recurso de Oracle
- Realice el backup del recurso de Microsoft SQL Server mediante el plugin para Microsoft SQL Server
- Realice un backup del recurso de Oracle con el plugin para bases de datos de Oracle
- realice un backup del recurso personalizado mediante el plugin para aplicaciones personalizadas
- Configure la base de datos SAP HANA
- Configurar la base de datos Oracle
- Restaurar un backup de base de datos de SQL
- Restaurar el backup de una base de datos de Oracle
- restaurar un backup de aplicación personalizada
- Cree un recurso SAP HANA
- proteger un recurso personalizado mediante el plugin para aplicaciones personalizadas
- Proteger un recurso de Microsoft SQL Server mediante el plugin para Microsoft SQL Server
- Modificar un recurso de Microsoft SQL Server protegido
- Quitar la protección del recurso de Microsoft SQL Server
- Proteger un recurso de Oracle con el plugin para base de datos de Oracle
- Modificar un recurso de Oracle protegido
- Quite la protección del recurso de Oracle
- clonar un recurso desde el backup mediante el plugin para una aplicación personalizada
- Clone un volumen de aplicación de Oracle desde el backup con el plugin para base de datos de Oracle
- Clonar un recurso de Microsoft SQL Server desde el backup utilizando el plugin para Microsoft SQL Server
- Crear un ciclo de vida de clon de un recurso de Microsoft SQL Server
- Modificar el ciclo de vida de un recurso de Microsoft SQL Server

- Elimine el ciclo de vida de un clon de un recurso de Microsoft SQL Server
- Mover una base de datos de Microsoft SQL Server de un disco local a un LUN de NetApp
- Crear un archivo de especificación de clon para una base de datos de Oracle
- Iniciar un trabajo de actualización de clones bajo demanda de un recurso de Oracle
- Cree un recurso de Oracle desde el backup con el archivo de especificación del clon
- restaura la base de datos en la réplica secundaria y vuelve a unir la base de datos al grupo de disponibilidad
- Cree un recurso de volumen de aplicaciones de Oracle

Completos

Puede usar las API para realizar diferentes operaciones.

- recuperar los detalles del backup por nombre, tipo, plugin, recurso o fecha
- recupere todos los backups
- recupere los detalles de la copia de seguridad
- cambiar el nombre o eliminar backups
- montar el backup de Oracle
- Desmonte un backup de Oracle
- catalog un backup de Oracle
- uncatalog un backup de Oracle
- obtener todos los backups necesarios para montar para realizar una recuperación de un momento específico

Clones

Puede usar las API para realizar diferentes operaciones.

- Crear, mostrar, modificar y eliminar el archivo de especificación del clon de base de datos de Oracle
- Mostrar la jerarquía de clones de bases de datos de Oracle
- recuperar detalles de clones
- recuperar todos los clones
- eliminar clones
- Recuperar detalles del clon por ID
- Iniciar un trabajo de actualización de clones bajo demanda de un recurso de Oracle
- Clone un recurso de Oracle desde el backup con el archivo de especificación del clon

División de clones

Puede usar las API para realizar diferentes operaciones.

- estime la operación de división de clones del recurso clonado
- recupere el estado de una operación de división de clones

- inicie o detenga una operación de división de clones

Grupos de recursos

Puede usar las API para realizar diferentes operaciones.

- recuperar detalles de todos los grupos de recursos
- recupere el grupo de recursos por nombre
- crear un grupo de recursos para el plugin para una aplicación personalizada
- Cree un grupo de recursos para el plugin para Microsoft SQL Server
- Cree un grupo de recursos para el plugin para base de datos de Oracle
- modificar un grupo de recursos para el plugin para una aplicación personalizada
- Modificar un grupo de recursos para el plugin para Microsoft SQL Server
- Modificar un grupo de recursos para el plugin para base de datos de Oracle
- Crear, modificar o eliminar el ciclo de vida de un grupo de recursos para el plugin para Microsoft SQL Server
- realice un backup de un grupo de recursos
- ponga el grupo de recursos en modo de mantenimiento o producción
- quitar un grupo de recursos

Normativas

Puede usar las API para realizar diferentes operaciones.

- recuperar los detalles de la política
- recuperar los detalles de la política por nombre
- eliminar una política
- cree una copia de una política existente
- crear o modificar la política para el plugin para aplicación personalizada
- Cree o modifique una política para el plugin para Microsoft SQL Server
- Cree o modifique una política para el plugin para base de datos de Oracle
- Cree o modifique la política para el plugin para base de datos SAP HANA

Reducida

Puede usar las API para realizar diferentes operaciones.

- recuperar todos los recursos compartidos
- recupere un recurso compartido por nombre
- crear o eliminar un recurso compartido
- recupere los detalles de almacenamiento
- recupere los detalles de almacenamiento por nombre
- crear, modificar o eliminar un almacenamiento

- detectar recursos en un clúster de almacenamiento de
- recuperar recursos en un clúster de almacenamiento de

Share

Puede usar las API para realizar diferentes operaciones.

- recuperar los detalles de un recurso compartido
- recuperar detalles de todos los recursos compartidos
- cree o elimine un recurso compartido en el almacenamiento
- recupere un recurso compartido por nombre

Complementos

Puede usar las API para realizar diferentes operaciones.

- enumere todos los plugins de los plugins de un host
- Recupere un recurso de Microsoft SQL Server mediante una clave
- modifique un recurso personalizado mediante una clave
- quitar un recurso personalizado mediante una clave
- Recupere un recurso de SAP HANA mediante una clave
- Modifique un recurso de SAP HANA mediante una clave
- Quite un recurso de SAP HANA mediante una clave
- Recupere un recurso de Oracle con una clave
- Modifique un recurso de volumen de aplicaciones de Oracle mediante una clave
- Quite un recurso de volumen de aplicaciones de Oracle mediante una clave
- Realice el backup del recurso de Microsoft SQL Server mediante el plugin para Microsoft SQL Server y una clave
- Realice un backup del recurso de Oracle con el plugin para base de datos de Oracle y una clave
- realice un backup del recurso de la aplicación personalizada mediante el plugin para una aplicación personalizada y una clave
- Configure la base de datos SAP HANA mediante una clave
- Configure la base de datos Oracle con una clave
- restaurar un backup de aplicación personalizada mediante una clave
- Cree un recurso SAP HANA
- Cree un recurso de volumen de aplicaciones de Oracle
- proteger un recurso personalizado mediante el plugin para aplicaciones personalizadas
- Proteger un recurso de Microsoft SQL Server mediante el plugin para Microsoft SQL Server
- Modificar un recurso de Microsoft SQL Server protegido
- Quitar la protección del recurso de Microsoft SQL Server
- Proteger un recurso de Oracle con el plugin para base de datos de Oracle

- Modificar un recurso de Oracle protegido
- Quite la protección del recurso de Oracle
- clonar un recurso desde el backup mediante el plugin para una aplicación personalizada
- Clone un volumen de aplicación de Oracle desde el backup con el plugin para base de datos de Oracle
- Clonar un recurso de Microsoft SQL Server desde el backup utilizando el plugin para Microsoft SQL Server
- Crear un ciclo de vida de clon de un recurso de Microsoft SQL Server
- Modificar el ciclo de vida de un recurso de Microsoft SQL Server
- Elimine el ciclo de vida de un clon de un recurso de Microsoft SQL Server
- Crear un archivo de especificación de clon para una base de datos de Oracle
- Iniciar un ciclo de vida de clon bajo demanda de un recurso de Oracle
- Clone un recurso de Oracle desde el backup con el archivo de especificación del clon

Leídos

Puede usar las API para realizar diferentes operaciones.

- recuperar informes de operaciones de backup, restauración y clonado para sus respectivos plugins
- agregar, ejecutar, eliminar o modificar programaciones
- recuperar datos para los informes programados

Alertas

Puede usar las API para realizar diferentes operaciones.

- recupere todas las alertas
- Recuperar alertas por ID
- Eliminar varias alertas o eliminar una alerta por ID

RBAC

Puede usar las API para realizar diferentes operaciones.

- recuperar detalles de usuarios, grupos y roles
- agregar o eliminar usuarios
- asigne un usuario al rol
- anular asignación de usuario del rol
- crear, modificar o eliminar roles
- asignar grupo a un rol
- anular la asignación del grupo de un rol
- agregar o eliminar grupos
- cree una copia de un rol existente
- asigne o anule la asignación de recursos al usuario o grupo

Configuración

Puede usar las API para realizar diferentes operaciones.

- ver los ajustes de configuración
- modifique las opciones de configuración

CertificadosConfiguración

Puede usar las API para realizar diferentes operaciones.

- Vea el estado del certificado para SnapCenter Server o el host del plugin
- Modifique la configuración del certificado para SnapCenter Server o el host del plugin

Repositorio

Puede usar las API para realizar diferentes operaciones.

- recupere los backups del repositorio
- se puede ver la información de configuración sobre el repositorio
- Proteja y restaure el repositorio de SnapCenter
- Desproteger el repositorio de SnapCenter
- reconstruir y conmutar por error el repositorio

Versión

Puede usar esta API para ver la versión de SnapCenter.

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.

Antes de empezar

- 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

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

"Aviso para SnapCenter 6.2"

Información de copyright

Copyright © 2026 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.